Tor

From the Dark Web to the Future of Privacy

Ben Collier

TOR

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

TOR

From the Dark Web to the Future of Privacy

BEN COLLIER

The MIT Press
Cambridge, Massachusetts
London, England

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

© 2024 Massachusetts Institute of Technology

This work is subject to a Creative Commons CC-BY-NC-ND license.

This license applies only to the work in full and not to any components included with permission. Subject to such license, all rights are reserved. No part of this book may be used to train artificial intelligence systems without permission in writing from the MIT Press.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Adobe Garamond and Berthold Akzidenz Grotesk by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data is available.

ISBN: 978-0-262-54818-2

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Contents

Acknowledgments *vii*

INTRODUCTION: ONION AND ON AND ON *1*

1 PRIVACY WORLDS *9*

2 THE WORLDS OF THE INTERNET INFRASTRUCTURE *25*

3 TOR'S STRANGE BEGINNINGS *37*

4 DESIGNING THE ONION *51*

5 ENTER THE MAINTAINERS *77*

6 THE ONION GROWS ROOTS *97*

7 THE DARK NET RISES *123*

8 THE ACTIVISTS *149*

9 FACING WORLDS *173*

10 PRIVACY FUTURES *193*

AFTERWORD *209*

Notes *211*

Index *227*

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Acknowledgments

My heartfelt thanks go out to my supervisors, Richard Jones and James Stewart, and my PhD examiners, Gabriella Coleman and Alastair Henry. They enormously shaped the ideas in this book. Thanks additionally to the reviewers, editors, cover artist, and everyone at MIT Press for their work and support on this book.

Thanks to all the people whom I interviewed for this project and to the Tor community as a whole. I am deeply grateful to Nick Mathewson and Roger Dingledine for their extensive comments on the manuscript, and to Paul Syverson, Shava Nerad, Steven Murdoch, Isis Lovecruft, and Isabela Fernandes for conversations about Tor and the book over the last year. I am also enormously grateful to Sarah Jamie Lewis, whose thoughts on *privacy as a structure* were vital in unlocking the rest of the ideas in this book. While I wish to preserve their anonymity, special thanks go to some of my interviewees in particular (you know who you are) for some dynamite quotes—living up to the long hacker tradition of speaking in parables.

I am hugely indebted to the Cambridge Computer Lab—particularly to Alice Hutchings, Ross Anderson, Richard Clayton, and Alastair Beresford, who were amazing mentors, and to all my postdoc pals (especially Lydia Wilson, who helped me improve my writing, and Daniel R. Thomas, who did the same for my programming). The Lab has played a huge role in Tor's history (something I only really understood after I left) and it was an enormous privilege to be part of it. Thanks also to my wonderful colleagues at STIS in Edinburgh for your support throughout the process of writing

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the manuscript. Solidarity to Shane Horgan, Louise Brangan, and Ben Matthews—who gave me tons of support throughout the PhD and since.

Finally, thanks to Jamie—for everything. But especially for reading the book dozens of times and contributing several of the key ideas.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

INTRODUCTION: ONION AND ON AND ON

I'm sitting in a cold, scuffed, and dirty plastic chair on a crowded train, watching freezing fog stream past the window—one of the many unpleasant but strangely enjoyable everyday experiences of life in the United Kingdom. Despite the train carriage hailing from the mid-1980s, there is something resembling Wi-Fi service, and so I connect, hoping to sneak in a few hours of PhD research. I load up the website of the Tor Project—or so I think—but instead reach a block screen courtesy of the train's Wi-Fi provider.

> Virgin Trains
> THIS WEBSITE IS PROHIBITED AND CANNOT BE ACCESSED
> REASON: CENSORSHIP CIRCUMVENTION

Sighing, I load up the Tor Browser and type in the address. The website loads instantly.

Tor—still known to most as the *Dark Web* or *Dark Net*—is not an easy subject to research. It exists on a bizarre terrain, simultaneously in the living rooms of lovely nerds, in the nightmares of police officers, in the small spaces of everyday digital life, and in the corridors of global power. It is a thin and brittle network stretched across the globe like a glass spiderweb and at the same time a profound challenge to the most powerful spy agencies in the world.

Even the basic facts of Tor can seem confusing. Explained simply, Tor is an infrastructure built on top of the internet that gives people very strong security and privacy protections online. It uses a clever technical design to

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

work around some of the most basic protocols and technologies that allow the internet to get your web traffic from one place to another. Regular internet traffic needs the digital equivalent of the to and from address on a letter in order to navigate to its destination, and these can be recorded by parts of the infrastructure your traffic passes through as it travels around the world. This has created a range of points at which the people who own and run the infrastructure in different countries have installed powerful tools for surveilling the people who use it.

Tor has a technological design that tries to solve this problem—to allow you to use the internet infrastructure without the infrastructure itself seeing what you're up to. This is no mean feat—the equivalent of getting a letter successfully to its destination with the *to* and *from* addresses being completely invisible to the post office. By doing this, Tor protects its users (although not absolutely) from the most powerful actors watching the internet today, including nation-states, police, spy agencies, and the massive private companies that run it.

Most users access Tor in the form of a rather innocuous web browser—much like Chrome, Safari, or Firefox—that rapidly clicks and whirrs through a pleasing set of additional messages before it starts up, giving it a slightly hacker-film feel. Once this is finished and the connection to the Tor network is confirmed, the user can simply browse the internet as normal.

But under the surface, the way their computer navigates the internet infrastructure has changed. When their web traffic reaches their internet service provider, instead of going to their destination site directly (which can then be logged by the provider and passed to secret services, corporations, and others who want to surveil them), that web traffic enters the dense thickets of the Tor network, composed of thousands of servers hosted by volunteers all over the world. After bouncing around the network to further confuse any prurient onlookers and shake off any tails they might have acquired along the way, the traffic reaches its desired destination—and the state spy agencies are none the wiser. This clever design means that Tor users experience the internet with drastically reduced surveillance and censorship, and the internet infrastructure itself can no longer track them.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Tor was built in the early 2000s from a design created by a team of researchers in the US Naval Research Laboratory, and has existed amid the swirls and clashes of the early internet cultures ever since. Even today, it remains at the frontlines of the battles between different visions of the internet's future—and its relationship to nation-states, to power, and to resistance.

Tor is packed full of paradoxes and contradictions, and so the surrounding public and academic debate is still fairly confused. Despite posing what seems to be a clear challenge to government power in the internet age, Tor has been outright banned by very few nations (and no democratic ones). In fact, not only were the technologies at its core originally designed within the US Navy but also Tor has received substantial funding from the US government for most of its life.

Funding a technology designed to resist government surveillance might seem an odd move for the United States—a country revealed in 2013 to have been conducting mass surveillance on its citizens and people around the world. But even deeper conflicts complicate what Tor means today—perhaps none more so than its use for crime. Tor is the technology underpinning the so-called *Dark Web*, an archipelago of anonymous online sites that use a feature of the Tor network called 'onion services' to prevent law enforcement from taking them down or identifying them or their users, thus protecting a trade in illegal products and services. Newspapers and politicians naturally focus on this, depicting the Dark Web as the internet's nightmare twin, a digital underworld where terrorists, drug dealers, and child abusers congregate outside the reach of law enforcement.

And yet, Tor is also a crucial weapon in the arsenal of law enforcement, journalists, and activists. It is used by investigators for cybercrime research, by newspapers to safely contact sources, and by human rights defenders to organize resistance. As Russia blocked access to the BBC in early 2022, the network promoted its own onion service—a mirror of its reporting in Russian and Ukrainian but hosted on the Tor network, and thus much harder for the Kremlin to censor—and Twitter spun up its own onion service as well. In practice, Tor has survived for more than twenty years in a rather

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

shaky relationship with the US government, supporting American global soft power by changing the online rules of the game in authoritarian nations, allowing the public to access Western news and social media and helping antigovernment activists there to communicate securely. For those trying to do hard, dangerous work resisting authoritarian power (wherever it might be emerging), Tor is one of the only ways to stay safe online, turning the internet from a tool of control to one of resistance.

Even stranger is what lies at the beating heart of Tor, protecting all these astonishing users, many of whom seem to have walked off the screen of a blockbuster action film. At its core is a vast crowd of more-or-less ordinary (if often slightly paranoid) people who use Tor simply to live their day-to-day online lives. Far from the raging debates about guns-for-hire, drug dealers, activists, journalists, and spies, most of Tor's users simply use it to browse the internet, experiencing something more akin to what the internet might have looked like in the 1990s (at least in the visions of the utopian technologists who did so much to create and promote it).

This book is a biography of the Tor network, stretching from when engineers and hackers first built the foundations of the internet in the early 1960s to the present day. It maps over these sixty years the cultural and technical ideas that have shaped what privacy has meant for different people at different points throughout the life of the internet, and how these formed and funneled into the cultures that have defined Tor. It also tells the complex and at times bizarre story of the Tor Project: how military scientists and underground hackers came together in the 1990s, at the height of the Crypto Wars, to build a technology that would reclaim the internet as a private space, and how their work was taken up and transformed by a changing world over the next twenty years.

There are two sides to this history. One is a history of privacy in the internet infrastructure and an attempt by a group of engineers, volunteers, and activists of different kinds to reshape the world. It maps the different visions of privacy that have proliferated in hacker cultures and how they shaped Tor as a technology—its design, how its network grew, and the alliances it made. While many think of the Tor community as a single entity—often a caricature of grungy techies steeped in cyber-libertarian politics—in fact, it

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

is home to a range of different cultures and values, all of which have changed substantially over the years. Those cultures and values have played important roles in shaping the technical design of Tor, the decisions and controversies that have defined its history, and the different ways it might shape the future of the Internet.

Fitting alongside this history of Tor itself is a wider story, one of the evolving shape of global power and a changing and mutating internet. Tor has been profoundly molded by these wider currents of change, from the internet's early roots in military communications to its rise as part of American neoliberal statecraft on the world stage, through the nightmare of the War on Terror, the utopianism of the Arab Spring, and now what seems more and more like the crumbling of global American dominance. But Tor has not only had a front row seat to these conflicts—it has itself played a crucial role in them.

Outside of global struggles, Tor has been equally central to the evolving domestic issues of crime and harm posed by the internet. As new terrains of online harm have emerged, from petty scams to coordinated harassment, from disinformation to online drug dealing, and from botnets to nation-state hacking campaigns, governments have tried to reestablish control of an online space that often seems to overflow with new threats.

Although governments have been quick to point the finger at Tor as an online den of iniquity, they have generally hesitated to ban it outright. To make sense of all this, any history of Tor must also be a history of state power in the internet age. This kind of history operates on a much broader scale than the conflicts and culture wars within Tor itself, but it is also at heart a story of culture and ideas, and how they evolve, change, and clash over time.

Together, these two histories provide some insight into the controversies that have dogged Tor throughout its life and shed some light on what its future might look like. Of particular interest to academics, policy makers, and police is Tor's (rather unfair) image as the defining technology of online crime. The Dark Web first burst into the global popular imagination with the rise of cryptomarkets, online spaces that repurpose the Tor network to make illicit commercial platforms that can hide where they are being hosted, and are thus very hard to censor or take down. Combining Tor with the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

ability to evade financial regulation offered by Bitcoin and other cryptocurrencies, the cryptomarkets created a new kind of commerce—a version of online marketplaces and forums that could operate totally free from oversight by governments or police.

Media depictions of lawless markets for drugs, guns, child sexual abuse material, and terrorist content captured the imaginations of the public. Since then, coverage of the Dark Web has been a reliable money-maker for journalists and documentary crews, eventually becoming the subject of its own cyber-focused niche of crime reporting. In the world of literary fiction, the Dark Web has become a shorthand for online deviance, mentioned in everything from William Gibson novels to spy dramas. Generally, it's seen as a place where anything is for sale, a digital Wild West that embodies society's broader fears of the large-scale social change and confusing, hard-to-pin-down forms of harm that have accompanied the internet age.

In fact, much of this is decidedly overblown, particularly reports of hitmen-for-hire services, which are more or less completely apocryphal. If you're out to buy drugs or have someone assassinated, it is still far easier for most people to travel to a major city and hang around in local bars than it is to do this online, let alone via Tor. In both cases, you'll get ripped off more often than not, but at least in the former you'll have soaked up some local culture as well, and possibly knocked back a few beers and made some friends. The truth about the Dark Web is actually a lot more interesting than the picture painted in popular accounts; the illegal marketplaces and forums hosted on the Tor network are pretty niche, but they have adapted to the difficulties of anonymous trading in some fascinating ways.

As a result of this widespread coverage of the so-called Dark Web, explaining Tor to others can quickly become an exercise in frustration, not helped by a fractured public discussion around Tor, cybercrime, and online privacy more generally. In particular, people often ask *why Tor is allowed to exist*, let alone be funded by the US government. The way that this discussion is usually presented is to weigh "good" and "bad" use cases against each other—for example, arguing that although some "bad" people use cryptomarkets to exchange prohibited goods, other "good" use cases abound, such

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

as journalists speaking to sources or activists organizing the overthrow of authoritarian governments.

I've always felt that this balancing act rather misses the point. Someone visiting a cryptomarket to buy off-script estrogen or birth control pills (as some do) or, for that matter, purchasing ecstasy in a safer, more regulated environment than off the street, is, to many, a "good" use of Tor. Equally, Russian state assets leaking disinformation to conspiracy theorist online publications, neo-Nazis using Tor to evade censorship, or QAnon adherents attempting to overthrow the US government seem like less desirable outcomes, even though they involve liberalizing control over communications.

Tor does something more radical: it reaches to the heart of contemporary forms of digital power and rewrites them. In contemporary digital societies, control of the network infrastructure is a profound source of both hard and soft power. The cold technical networks that route signals around the world dictate which communications go where and who can surveil and censor them. What Tor does is to radically reorder these power structures of the internet. This form of hard control opens up a range of channels for soft power, changing the flow of communications to allow different actors and narratives to thrive.

The United States and its allies are no stranger to laying an infrastructural and technical foundation for liberal market democracy, even by force. Much as the BBC World Service and Radio Free Europe played key roles in the Cold War, Tor serves as a strategic asset for Western soft power. This is not to say, as some do, that Tor is a shadowy "information operation," a honeypot for security services, or, conversely, simply a neutral technical project without any politics at all. Having spent years reading through tens of thousands of Tor's documents and spending a lot of time with members of the Tor Project, I have found little evidence for any of these claims. Instead, much like any of the massive digital infrastructure projects we are watching reshape the world around us, Tor unites a wide range of different interests and groups, some of which directly oppose one another. It does this through a kind of structural politics—a technical design that goes some way toward solving many of the issues that a wide range of different groups have with the internet.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

But, as I argue in this book, structure isn't enough on its own. In fact, since Tor was designed in the 1990s, it has taken years of work by thousands of people to make and maintain Tor as a reality—to keep developing it, securing it against new threats, maintaining its extensive digital infrastructure, and helping it grow and adapt to the changes in the internet and how we use it over the last twenty years. And huge amounts of hard work have gone into getting Tor to the people who might benefit from it—telling them it exists, showing them how to use it safely, ensuring that it stays funded and remains legal. Without this work, Tor would collapse, or at most remain a hobby project for a small group of American and European tech nerds.

This places the people who make Tor work—the Tor community itself—in a very odd position, balanced between many different levels of digital power. These people and their cultures are a crucial part of making sense of what Tor is and the role it plays in the world. This book is their story—or a small part of it. It is the story of how a technology of resistance was born deep at the heart of power. It is the story of an odd, mismatched community of engineers, maintainers, and activists. And finally, it is the story of how one of the biggest hacks ever was carried out—and is still happening—at the core of the internet itself.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

1 PRIVACY WORLDS

Before embarking on the history of Tor, it is worth discussing two key ideas behind it: *privacy* and *digital infrastructure*. To understand what Tor is and the role it has played in the world, we first need to understand a bit about how the internet works and what this means for privacy in the societies that depend on it.

Although privacy is one of the main concepts that we rely on to discuss digital technologies today, it remains a rather nebulous one. Privacy "concerns" and "issues" dominate public debates, but rarely seem to resolve into specific instances of harm except in rare cases, which themselves often serve more to demonstrate misuse of a system rather than a fundamental problem with the system itself.

For example, reactions to mass surveillance systems often focus on the fact that they scoop up vast quantities of data from the population as a whole, but overlook that they are overwhelmingly used to target minority ethnic and religious groups in particular. Here, as Seda Guerses, Arun Kundnani, and Joris van Hoboken argue, evoking privacy en masse is often used to *justify* targeted forms of surveillance against minorities, as long as the wider privacy violation against the majority is corrected.[1] The concept of privacy is further deployed with a vast array of different meanings in different contexts, making it hard to pin down as a single argument.[2]

Despite some of the shortcomings of privacy as a concept, it's still a vital tool for understanding power in digital societies. In reality, privacy is deeply linked to power and politics. Privacy gives us a framework for thinking about

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the creation and demarcation of different kinds of space. It sets out the spaces where different rules and forms of power apply: the private home, the public sphere, the temple, or the market. It is not just about information but rather about what rules apply where and to whom, and who gets to enforce them.

In contemporary societies, where multiple systems of power overlap around each of us, these spaces are often embedded with or built on digital infrastructures. They require a slightly different way of thinking about power and practices than did the technologies that have historically demarcated private spaces—for example, walls, cars, confession boxes, windows, bank vaults, and sealed letters.

Let's begin by considering what privacy might look like in a digital society. In the popular imagination, we might imagine a young person sits reading at her computer in her bedroom at night with a dozen tabs open in her web browser. This is undeniably a private space. The tiny fortress of the dark bedroom lies nested within the larger familial bounds of the private home.

When this person and her friends are depicted in the media, the article or news package usually shows a darkened room, the person's face lit up by the blue light of their mobile phone or laptop monitor. It's worth noting here that this perfectly private physical space is hypothetical and isn't accessible or even recognizable to many. If our young person was sharing a bedroom with a sibling, lived with a family who insisted she keep the bedroom door open, or lived in another shared setting—perhaps an immigration detention center, refugee camp, prison, or any form of communal housing—then the kinds of space and privacy she might be able to find or create would be radically different. Her access to privacy might be shaped by material factors—what the walls are made of, for example, and how much they block light and sound—or by norms dictating what practices are deemed common or acceptable (for instance, closing a door to denote a wish not to be disturbed). Furthermore, there might be very different expectations, values, and basic ideas of what privacy means and how it interacts with other aspects of culture—ideas about growing up and what it means to be a teenager, about acceptable parenting practice, or about nudity, sex, and relationships. Even in this example, the basic ideas of what constitutes privacy are deeply contingent on culture and context.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Within these nested spaces, her computer and mobile phone might contain deeper levels of privacy still. Like a combination of a diary, a telephone, and a loudspeaker, they involve the most intimate and the most public kinds of interactions and communications imaginable. In one window, she's chatting to her friends on Discord; in another she is deep in a Wikipedia rabbit hole, and still other windows host YouTube playlists and Netflix films paused halfway through.

It's worth considering here the material aspects that emerge at this level—we might think of this as the digital equivalent of the thickness of the walls of the room and how well they block sound. When she tries to visit a website—say, the *New York Times* home page—her computer searches the name of the website, accessing the global Domain Name System (DNS), which translates it from www.nytimes.com into an IP address that the internet backbone can read—something like 151.101.125.164. It then sends a signal to the nearby router, which logs the timings of the signals that it receives from the various devices in the house. The router passes the traffic down a cable to a local switching station that then sorts the traffic into flows and hands these off to the local server hubs of the internet service provider (ISP) that manages her internet access. These hubs exist in all major cities, establishing outposts of internet infrastructure through which customers can be linked up to the wider internet.

As this web traffic passes through data centers belonging to ISPs, key details including the destination, origin, and timing of the signals are noted and, in many cases, retained for future review. The ISP has a list of IP addresses associated with particularly harmful sites provided in part by government agencies, its own policies, and a network of volunteer administrators working behind the scenes. If, as happens in many countries, the government wants to block a website, it simply asks the ISP to add, for example, Facebook's servers to a blocked list. The ISP can then simply refuse to allow the traffic to reach Facebook servers.

Often, cooperation will go even farther. The ISP will watch for particularly suspicious activity, hand over traffic records to intelligence agencies, or work with law enforcement that has seized a computer or identified a suspect and want to know all the websites the user has visited recently. The

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

ISP usually can't see the content of your online interactions—the messages that you type into a chat program and the content of the pages you visit are generally protected by strong encryption—but they do see who you're talking to, where you're visiting, and when. This alone can be very revealing.

People often think that the internet is flat—that once you get past the ISP, the entire thing opens up like the Matrix, a vast hyperspace. But a lot of work goes into maintaining this illusion—in reality, the internet has a geography all of its own. The ISP takes a user's signals and routes these up to a bigger network of networks, a large area of internet routing infrastructure called an AS, or Autonomous System, of which there are around 37,000 in the world. These ASes form a landscape of their own, linking the physical servers of the internet backbone together into their own constantly shifting digital geography. The ASes build links with one another via a range of arcane processes conducted in their own language, called BGP, or Border Gateway Protocol, which allows them to see what the day-to-day landscape of the internet looks like, and to identify how to get signals to their eventual destination, between the respective sectors of the internet that they each manage.[3]

ISPs, ASes, and other actors involved in internet administration exert an enormous influence on the macro-scale flows of data around the world. Although our young internet user might be accessing the *New York Times*, whose home servers are in the United States, the ISP won't even bother sending her requests to see the newspaper's home page all the way there. Even at the speed of light, that would take too long. Instead, most of her communication is with much closer hubs, called the *edge network*, that periodically download copies of big chunks of the internet.

Far from a "neutral" internet, the ISP bandwidth used by her and other people trying to reach commonly browsed websites like the *New York Times* is far greater than that for people trying to reach small, seldom-visited paths on the internet, such as self-hosted cooking blogs.[4] This physical geography of the internet is much more managed, complex, and hierarchical than the myth of the flat, densely interconnected network would suggest, and it creates data bottlenecks all over the place. From the undersea cables transmitting data between continents, to the networks of links between the ASes and the data centers and local networks we rely on, the internet is full of places

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

where governments, spy agencies, and even infrastructure companies can get a pretty good picture of what's going on with a handy snooping device or wiretap.[5]

The sites that our teenager is visiting are themselves gathering their own data, as well—not at the low levels of physical infrastructure, but way up in the stack on the levels we actually inhabit day-to-day, in the realm of websites, apps, and services. The browser she uses to navigate the internet is downloading a range of trackers on many of the websites she visits. And most of the commercial services she logs into, such as Facebook, Netflix, Amazon, and Google, are keeping a record of what she says, buys, and watches.

In her bag, nestled next to AirPods and house keys, is her mobile phone—increasingly our preferred method to engage with this huge digital infrastructure. It, too, collects a range of data through apps, location trackers, and even heart-rate monitors in connected smart watches, and it feeds that information to centralized servers owned and analyzed by private companies. Even if you block all these data sources, websites can use the unique combination of fonts, software, hardware, and settings on your machine to track who you are by way of a technique known as "fingerprinting."[6]

This vast network of surveillance and management isn't just passively blocking and watching traffic as it goes by; it is also used to actively shape our lives, controlling what we see, what we do, and even who we are. This massive infrastructure of data collection creates a set of new spaces of power where messages can be designed, injected, and modulated in (or deleted and censored from) the data stream, permitting powerful actors to shape culture and behavior for a fee.

All of this data about our hypothetical teenager is used to build profiles of her interests and browsing patterns. These novel sources of digital data are then connected by the advertisers with more traditional but no less powerful data sources. These come from corporate databases, often collected by marketing companies through surveys, censuses, and commercial and government data they purchase.

Together, all these different sources of public and private data are used to stitch our hypothetical internet user—accessing the internet from the supposed privacy of her home—into a dense map of people, beliefs, and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

demographic profiles that can be used to shape and nudge her behavior through hypertargeted advertising. This is a crucial point in debates around internet privacy—it's not just about controlling our data and where it goes for its own sake but rather how that control is used to influence and exert power over us.

Initially, digital privacy activists were concerned primarily that such broad data collection would give private companies a wealth of ways to control and exploit us through data-driven commercial marketing. Then, the Cambridge Analytica scandal revealed to the public that the techniques and tools of targeted digital marketing were also being used by private contractors and think tanks to interfere in elections and spread propaganda.[7] As more and more people gained access to the digital advertising infrastructure, crime groups began to exploit it, too, using it to advertise illegal services, spread malware, and promote scams. Finally, in recent years, it has become increasingly clear that governments and law enforcement are now using intimately targeted behavioral advertising to "nudge" our behaviors and shape our cultures based on who we are, where we are, and what we are doing online.[8]

Thus, what we do in the private space of the bedroom is broken up and transmitted around the world. What we thought was accessible to only ourselves ends up in the hands of the powerful. With Tor, however, this scene plays out rather differently.

If our hypothetical teenager uses Tor, the web traffic leaves her computer, still heading to the ISP, but all the ISP sees is that the traffic is heading into the Tor network. There, it bounces around the world through a succession of relay servers, the last of which serves it to the destination website. The Tor browser itself strips away many of the cookies, tracking pixels, and fingerprints that the internet giants and the websites we visit use to track us in the "upper layers." And to the internet infrastructure, her origin and destination IP addresses appear simply to be those of a random node in the Tor network. Her preferences, posts, and purchases are still logged when she signs into platform services like Amazon, Facebook, Twitter, or Netflix, but only when she chooses to allow that. And even then, that information can't be used to serve ads in the browser.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

In other words, she experiences a far more private version of the web, something more like the internet of the 1990s. While the user isn't outside the terrain of power entirely, she has far more control over what she sees and who sees her. Thus, the internet, rather than demolishing the privacy of the bedroom, creates a new space with radical new capacities, where the lines of power are radically redrawn so that the user may connect with others *on her own terms*, rather than on the terms of governments and internet companies.

Instead of returning to pre-internet forms of privacy, Tor does something much more powerful: it recreates the utopianism of the early internet pioneers, in which many users felt the connective power of the whole internet at their disposal. They experienced a global public sphere that was much harder for governments to control (even if with much of the poison that we see today).[9]

At this point, some readers, particularly those already familiar with the Tor Project, might ask whether *privacy* is really the most important concept for Tor. There are many values central to Tor—as a project, it's not just about privacy, but also anonymity, decentralization, openness, transparency, security, antihierarchy, freedom of speech, utopia, resisting censorship, and the classic hackery love and fear of computer technology.

These values, which stem from the cultures and ideas that have animated the Tor Project throughout its life, have all shaped what Tor is and how it works. They have all guided the development of Tor, leading to some design decisions over others. They have underpinned the public statements various contributors to the Project have made over its history, and each has shaped who has joined Tor and how they have spent their time. So why might we focus specifically on privacy?

Privacy is a foundational concept in human societies. It demarcates different kinds of spaces, activities, and ideas, within which different systems and structures of power operate. It is thus particularly important to liberal conceptions of democracy, in which it is understood as one of the central values underpinning democratic social life. In the classic liberal view, privacy represents restrictions on state power, keeping it away from spaces in

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

which commerce, politics, and individuality can germinate and be allowed to flourish independently.[10]

Thus is born the private business, the private home, and finally, the private political, emotional, and mental space of the individual. This is often framed as the "right to be let alone" by the state or the press.[11] In more mundane contexts, it can also be the right to be let alone by your neighbors, by your family, or by your partner.

On one level, privacy is—and always has been—about control over the flow of information. This is especially true in today's world, in which information technologies support so much of social life. We largely assess privacy by asking who has control over what information: Who knows what websites you're visiting? Who can see you going to the toilet? Who has access to your medical history?

But privacy isn't about information alone, and this becomes clear when it's broken. Underneath the ideologies and political arguments around privacy is a terrain of deep emotional reactions. Breaches of privacy, even relatively minor ones, are often accompanied by a deep sense of shame and embarrassment. Norbert Elias deals explicitly with privacy in his accounts of what he called the civilizing process—the increasing separation of different areas of life in modern societies, each with its own particular customs and norms, and increasingly complex divisions of power and protocol within them.[12] Privacy is, in practice, a very broad concept that bounds up the customs, values, and technologies that we use to demarcate and mediate these spaces of power.

Thus, Tor doesn't just provide secrecy by hiding the content of your communications through encryption. It doesn't just give you anonymity by hiding who you talk to and the sites you visit. It doesn't just allow you to bypass censorship by governments and corporations. In doing all these things, it does something much larger: it demarcates a separate space in which government and corporate control and power, whether exercised through influence, coercion, surveillance, or censorship, are removed from our private online lives. It gives us privacy in a very full and rich sense.

Privacy is not solely a liberal or Western idea. Understood more broadly, privacy (and similar ideas) is important in a range of political and cultural

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

systems. Although Western commentators love to claim that privacy simply doesn't exist in Chinese or Indian culture, for instance, analogous concepts are in fact important in most cultures (though not always between the individual and the state). As conceived in the Confucian philosophical tradition, for example, a range of related concepts exist, though these often operate at the level of the family rather than the individual.[13]

This is by no means unique to China and will be familiar to anyone who has grown up in a Western family or community in which patriarchal or religious values predominate over democratic and liberal ones. However, the legal definitions of privacy used in many countries and cultures around the world have often been imported from Western contexts rather than developed from culturally specific ideas of privacy. After all, even in places where a culture of privacy is well developed, when new technologies or laws developed elsewhere are imported, they often bring their own cultures with them, interacting with these new users' ideas of privacy in complex ways.[14]

Underpinning a particular idea of privacy is often a structure of power or authority—the patriarchal power structure of the "traditional" family, the power of God and religious elders, the authority of the private homeowner and private property, or the intimate forms of power that separate a person's innermost thoughts and feelings from the outside world and its structures of control.[15] Some forms of privacy, such as those that align with the dominant order of power, are given by those authorities, but others are taken from them—for example, the use of a secret language or code to render a message unreadable by the government.

As a concept, privacy nicely captures both the technolibertarian ideas important to Tor and other decentralized internet projects and the more radical, nascent possibilities. Focusing on privacy, therefore, allows us to view these concepts together—some about technical design, some about politics, and some about everyday human values and practices—and link them to an analysis of power.

The vision of privacy I describe above—the one most people experience—isn't a cold, abstract one merely drawn in a network diagram. It is messy and warm, found in cloisters and confessionals, bedrooms and bars, union meetings and urology appointments. Sometimes it empowers—the teenager

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

exploring who they are without the watchful eye of a parent, or a slip of paper passed under a table between co-conspirators. Sometimes it restricts or shames—the private space of the patriarchal home used to control access to public life for women and children, or the family's social standing which compels people to keep who they are or who they love a secret. Police have long used the private space of the home to render domestic abuse a "private matter" that fell outside of their mandate.[16] And although it is often conjured as part of an individualist capitalist politics (the private space defending one's thoughts from the government or one's property from the tax collector), privacy can also be part of more radical and communitarian practice, underpinning intimacy, solidarity, and shared experience or organization.

So when you try to create a particular kind of privacy in a certain situation, you also step into a broader culture and its structures of power. This cultural richness seems at first irreconcilable from the technical ideas of privacy rendered in the design of signaling systems or databases, expressed in math and code. But in reality, they are inexorably linked. Privacy scholar and information scientist Helen Nissenbaum proposed a radical way of thinking about digital privacy that includes these ideas of related culture and values, but also provides a useful set of tools for practical work with computer systems.[17] Nissenbaum argues that privacy is produced *in context* and that the norms associated with those contexts should travel with it. She calls this "contextual integrity." So when the data captured in your doctor's office travels around, it should carry with it the norms and values of the doctor's office.

This articulation of digital privacy takes older, richer ideas about privacy and translates them for a world that sees privacy solely through flows of information. Although it shows us how ideas about privacy might be realized in technological systems, it doesn't tell us much about how the reverse might be true—how the design of modern technologies might influence our modern ideas about privacy.

In addition to being abstract cultural concepts, privacy and anonymity are also deeply bound to the material and technical world. The privacy created within the private home, which is informed by particular social structures and cultural ideas, is also made possible by material technologies—the walls of the house, the doors and locks, and the layout of the rooms.[18]

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Technologies themselves have their own cultures and conventions of use that are linked to the material world in a range of different ways. Science and technology scholars have often talked about this as a process of *inscription*—we write our values into the technologies we build.[19] So if we want to understand Tor and how it has shaped the landscape of online privacy across its history, we might try to pick apart the privacy values of its designers to understand how those values have shaped it over the years.

Doing so is harder than it might seem at first. Going back to our example above, as internet technologies have spread throughout the world, they have brought with them radical new material orders of privacy. We understand intuitively that digital infrastructures are intimately bound up with material power, but the way in which that power manifests and operates in society is less clear. In contemporary digital societies, our understandings of power revolve more than ever around technology. As different actors have fought to claim different spaces of the internet as the domain of different systems of power, so too have our ideas of privacy—which regulate movement and boundaries between these systems—undergone a profound shift. This raises a crucial question: How do you exert power through and over infrastructure?

One way to think about this is through networks. The idea of the network is an old one but became popularized in the 1980s as a way of thinking about societies that were increasingly global, financialized, and mediated by computer technologies[20] This popularization is reflected in the writing of the period, with scholars visualizing late modern society as a plane of dense networks of technology, people, finance, and power. The webs and cluster diagrams used to illustrate these arguments give us a ready-made, visually compelling way of thinking about power in which one can *see* different modes of power represented in different network structures, from the centralized "spiky amoeba" funneling back to a single point to the decentralized networks that resemble dense root formations. When digital scholars talk about power, the metaphor of the network is often not far behind.

Network forms of power are hard and angular; there is little room for interpretation in the cold lines of a network diagram. They lead to a kind of structural determinism—the idea that to change society, all you need to do is reshape the network. In a similar mode, the work of technology studies

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

scholars Laura DeNardis and Francesca Musiani on digital infrastructure identifies power through the concentrations of lines in the network map, as the places where human and technical connections meet and the waypoints through which people, data, information, and money are forced to pass.[21] These control points can be thought of as the clusters on a network diagram where all the lines come together at a single node. If you want to get something done, you need to pass through them, and if you can get control of one of these nodes, you can exert a great deal of power.

Despite its utopian visions of a "flat" hyperspace, as we saw above, the internet infrastructure is full of these nodes or control points. For example, if you want a high-speed connection to the United States from Europe, your traffic will need to pass through the undersea fiber-optic cables that connect the two continents. This is a material aspect of the internet as a network.

If you could put a pair of high tech crocodile clips on these cables, you could exert an immense amount of power by, for example, reading and surveilling huge swaths of data about people's intimate lives.[22] So here, privacy might be a case not only of who gets to see your data but also of these clusters of control in the networks of digital technologies we use day-to-day.

Other kinds of network hierarchy are important too, beyond just the topology of the infrastructure. For example, we might represent the control that developers wield over the design of the technology—and thus the ability to change the code and force people to use it—as a particularly concentrated network of power. One step further up the chain, the CEOs and policymakers that tell these engineers what to do might represent another kind of network again. In contemporary digital societies, we move through these complex and contingent networks all the time, with people budding off and rejoining different systems of power as they engage with different parts of the digital infrastructure.

This view of network power can sometimes seem rather disempowering, with humans caught helplessly in the structures of technology. It is tempting to see the world this way: the designers and engineers with all-consuming power, and evil states and corporations concentrating power in hierarchies while plucky resistance projects redistribute power in decentralized networks. But this infrastructural power doesn't just flow in one direction.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Take a widely used technology such as WhatsApp, for example. The forms of privacy, communication, and community experienced by WhatsApp's billions of users around the world aren't solely determined by the decisions of a few engineers in Silicon Valley; the users themselves have substantial power to hack, subvert, and undermine the envisioned experience built into the technologies they use.[23] However, the designers of digital infrastructure do wield a lot of power—namely, setting the starting point and the paths of least resistance for what is possible.

As we will see in this history of Tor, there are other kinds of infrastructural power that exist outside of the network. The global networks of digital infrastructure rely on huge interlocking systems of technologies and people. Tor isn't just a tool—it's an entire infrastructure of its own, reliant not only on its designers but also on a wide range of other people and technologies. Without the extensive Tor network and the thousands of people who keep it running (and have their own ideas about privacy), the Tor Browser would not work. Without the developers continuously breaking and remaking parts of Tor—in a feverish arms race against the most well-resourced spy agencies in the world—it would be useless within months. And without enthusiastic activists traveling the world to tell people about Tor and how to use it safely, it would be doomed to the fate of niche and obsolete technologies such as the minidisc player or Betamax, restricted to a few tech nerds and nostalgia buffs. So our history of Tor needs to go beyond a history of its design and designers, to include a range of other cultures and perspectives. Although the material structure of the network is critical, the worlds of the infrastructure and technologies are as rich and messy as any other component of "privacy."

Bringing this all together, we arrive at a useful way of thinking about privacy and digital infrastructure: as something to be actively produced and maintained, both through continuous human work and social practices and through technologies, infrastructure, and designed spaces. The kinds of privacy we find in a doctor's office, in a lawyer's privileged phone call, in a confession booth, or in the bedroom are bound up with the *social worlds* of the people who make and inhabit these spaces.[24] The privacy experienced in each of these spaces derives from the values, practices, and technologies that support them.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The social world of the doctor, for example, draws on the long history of the profession; the cultures, knowledge, and practices internalized over years of training and work; the design of the hospital and the clinic; their legal and regulatory environment; and the wide array of different technologies used, from stethoscopes to scalpels. Within this world is a particular interpretation of privacy and a series of practices used to create it. In the case of the doctor, privacy can be found in the protection of patient records, in drawing a curtain around a hospital bed, and in the sacrosanct confines of a doctor's office.

The doctor alone doesn't create that privacy, however. They usually don't have the coding skills to make a secure patient records program, or the architectural know-how to build a hospital. Privacy exists at the intersection of the worlds of the patient and the doctor in the moment of the consultation but also the worlds of the architect who designed the surgery, the computer engineer who designed the patient notes program, and the administrator who manages the databases behind the scenes. Each of these deep cultures contain different ideas and conceptions of privacy, and each plays a unique role in creating the privacy that you actually experience as the patient. Taking the architect as an example, a consultation room with glass windows or an open-plan design might mean something rather different in terms of the privacy you experience.

This gives us a concept from which to write a biography of the Tor network: the concept of the *privacy world*. The first component of a privacy world is its ideas, values, and visions of what privacy means. Our teenager might see privacy mostly in terms of keeping her life hidden from her parents; our drug dealer might see it in terms of securing themselves against the police; and the system administrator might see privacy in terms of databases and records. These ideas are linked to the second component of a privacy world: the *practices* through which these people actually try to create privacy. For example, the drug dealers looking for privacy in the cryptomarkets might use fake names and package their products up in DVD cases, all while relying on the relay operators maintaining the nodes in the Tor network and the designers of Tor fixing bugs in the code. All of these practices need to work in conjunction to successfully realize the drug dealer's vision of a private space

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

to trade Bitcoin for heroin, even if they would be unlikely to share the values or culture with the technical workers behind the scenes of Tor.

The third, and final, component is the *material technologies and infrastructures* around which these privacy worlds cluster. These infrastructures—such as Tor, or the internet itself—form bridges between worlds, linking up the drug dealers with the privacy activists, the spies and the freedom fighters, the security consultants and the cryptographers. The digital infrastructures around which we build privacy worlds are themselves packed tightly with ideas about privacy, written into the code and protocols and realized in their technical design.

This last part—the infrastructure—is crucial. The advent of the digital age has meant that there are now many new worlds that delineate the boundaries between spaces of power in social life. In previous centuries, a similar position might have been held by architects, lawyers, or even police or spies. But now (in addition to these), the worlds of people who work with digital and networked technologies have come to the fore as some of the most influential in our societies. Across the twentieth and twenty-first centuries, this new class of tech workers has risen to power with its own very strong ideas about privacy. From the early military-academic researchers who first laid the foundations of the internet, through the boom of the World Wide Web in the '90s, to the social media princelings, the privacy values embedded in the internet have been shaped by the ideas of successive generations of people in charge of the infrastructure.[25] More recently, the world of the "crypto bros" has tried to sell its own vision of a hyperfinancialized future. Here we can see the power of some of these worlds—the obscure ideas and values of tech workers in San Francisco being shipped around the planet in the form of new digital infrastructures.[26]

Most of the stories that have been told about Tor to date have been histories of particularly compelling or unpleasant groups of users and the worlds in which they live—drug dealers on cryptomarkets, terrorists and pedophiles, freedom fighters, exiles, and hackers. Underlying all of these, however, are privacy worlds that have not been explored: those constructed by the people on whom the Tor network itself relies, including its builders, maintainers, and advocates.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

In writing this book, I interviewed more than thirty of Tor's core community members: its developers, the people who maintain the network, and the advocates who promote it around the world. I also spent several years at hacker conferences talking to the wider Tor community, and analyzed thousands of pages of emails, financial reports, code commits, design documents, and blog posts from Tor's vast online archives. Throughout this book, I illustrate Tor's biography with quotes from these interviews—mostly conducted between 2016 and 2022—and from more than twenty-five years of emails and documents, going back to Tor's roots in the US Naval Research Lab.

Tor seemed to me, a naive outsider, to be a technology with such an obviously political mission that I assumed it had a strong, uniting set of core beliefs—a single cultural world. Nothing could have been farther from the truth. When I began mapping out Tor's history and interviewing the people who make it work, I was immediately struck by the rich diversity of cultures and values within the Tor community. From one person to the next, the motivations, beliefs, politics, and even understandings of what privacy *was* seemed vastly different. Even within the same interview, I would often find my interviewees putting forward what seemed to me like contradictory understandings of Tor, talking first about Tor as a tool for activists that could give power to the voiceless, and then arguing that it had no politics at all. From these interviews, and across the history of Tor, I found three main *privacy worlds*—cultures of privacy that have developed over Tor's lifetime, and that are rooted in different parts of the core technologies and work on which Tor and its users depend. In the following chapter, I trace the roots of these three worlds through the early years of the internet.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

2 THE WORLDS OF THE INTERNET INFRASTRUCTURE

As I began researching Tor, it became immediately clear just how odd a technology it is. Every time I peeled away one layer of the "onion" by spending hours conducting interviews or reading archives, another set of paradoxes and contradictions would emerge. I found that the cultural life of Tor was embedded in a range of cultural movements that were far older than Tor itself, and in fact extended into the earliest history of the internet.

There is a great deal of research and writing on so-called "internet cultures," often focusing on the social movements, subcultures, and communities that have grown into and out of online spaces. Many of these groups owe their continued existence and influence to the connective power of internet infrastructure, and some have gone on to shape in profound ways how the rest of us use the internet today. But beneath those lie another set of cultures: those that have shaped the internet's technologies and infrastructures themselves. These are not so much cultures *on* the internet as cultures *of* the internet. These key cultural worlds have been the subject of a range of internet histories—of the military scientists who designed its early protocols, the government cryptographers of the Cold War, and the Silicon Valley social media giants, to name a few. These groups have not just shaped how we use the internet, but also what the internet actually is.

By exploring the history of the internet, we can see the ways in which larger cultural movements shaping its infrastructure have been funneled into and shaped the smaller-scale worlds that cluster around particular technologies like Tor. Although these early internet worlds weren't necessarily

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

centered around privacy the way Tor is, privacy was a crucial concept in their development, and they have all played parts in influencing the cultures surrounding Tor today. The emergence of Tor was thus just one chapter in the long history of competing visions of the internet.

The internet's roots are well-documented and can be traced back to the Advanced Research Projects Agency (ARPA), an agency of the US government founded in 1957 to carry out scientific and technological research projects for the Department of Defense.[1] ARPA and its contractors began developing the ARPANET computer networking project in 1967 as an attempt, using approaches developed by the RAND Corporation, to establish decentralized, nationwide computer communications in a hypothetical nuclear war scenario when centralized exchanges might be destroyed.

This Cold War context led to the development of a "distributed" network, a decentralized computer communications system that routed packets of information along different paths and assembled them at the destination without any need for a centralized authority. The scientific community (which itself was viewed as crucial to maintaining US military supremacy) and universities shared many of these aims and ideas, both of which adopted the internet early on to share computing resources between researchers nationally as well as to implement systems for more direct military use.[2]

Thus, the internet's foundational visions have their roots in the ideas, motivations, and perspectives of the US military and a research and technological elite based in US universities and research labs.[3] Thus, even today, at the heart of many of the foundational infrastructures of the internet lies a fusion of *military-academic* practices and cultures, even if they might be unrecognizable and invisible to most users.

Although personal privacy wasn't exactly at the top of these researchers' list of priorities, secrecy and security were important features from the start, as the data shared were mostly military and scientific in nature. This also wasn't occurring in a vacuum—it was the 1960s, and there was already a highly developed industry of government secret communications among the United States and its closest allies that included large networks of codebreakers and cryptographers, researchers developing secure communications systems for radio and telegram, and new spy agencies, including the US'

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Central Intelligence Agency (CIA) and the UK's Government Communications Headquarters (GCHQ).[4]

Strategic decentralization was another key concern for the early military-academic designers of the internet. Those designers, their priorities rooted in the politics of the Cold War, cared deeply about the strategic distribution of network power in the technical systems they were building. If the United States was going to be bound up within a global and domestic communications network, it had to be one in which they could exert control. They were committed to decentralization not as a value per se, but rather as a pragmatic interest of the US government, both domestically and in the sphere of geopolitical power. These scientists were designing systems to solve particular research problems determined by their funders in the military; rather than attempting to achieve a particular kind of system for its own sake, they were attempting to develop an infrastructure for the internet that could both be resilient and provide a topology that would allow the United States to establish itself at crucial control points.[5]

At the heart of this value placed on strategic decentralization was an idea, familiar to military strategists and engineers alike, that power is embedded in topologies of control. Attaining command of key control points, whether through the design of technical systems or crucial infrastructure like roads and power grids, is in both military and engineering worlds key to the exertion of power.

Deep in the heart of the early internet, this gave rise to an apparent contradiction: the highly centralized, hierarchical US military found its needs best met by a fundamentally decentralized design, one in which signals were routed without a centralized authority that they could control. A central exchange could be bombed or compromised, whereas a decentralized design would let signals route around damage like a living organism—the resilience of the system outweighed the benefits of centralized power. While this was happening, though, a counterculture had been developing among the communities of technical experts, researchers, and academics involved in designing networked computing, and in the hobbyist communities increasingly gaining access to these networks.[6] For these people and the movement growing around them, decentralization—and the radical changes to the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

social arrangements of power that it could bring—was a cause in its own right.

Despite their close engagement with the US military, the technologists and researchers who developed the early technologies of the internet held sensibilities that often ran counter to that of their more "establishment" bosses in government. Rooted in the counterculture of the 1960s and 1970s (though perhaps more "libertarian rather than liberational"), their ideas emerged both from computer science departments (especially the much-documented Tech Model Railroad Club and Artificial Intelligence Lab at MIT) and the countercultural movement in San Francisco.[7] They established a vision of technology in which the structural forms, design principles, and technical practices of information systems were themselves the embodiment of a particular politics: later called the "hacker ethic."[8] They mobilized the values of the protest movements against the Vietnam War and for the civil rights movement—values like anti-authoritarianism and liberation—and envisioned that those values would be reflected in the technologies they were building.

Hackers—expert computer technologists who could take systems handed down from above and repurpose them to new ends, or build entirely new ones of their own—emerged as the heroes of this libertarian utopia, epitomizing the futility of state attempts to dominate subjects through authoritarian technology. For the countercultural hacker world, decentralization was a political end in its own right, and one deeply bound to libertarian ideas of privacy as the freedom of the individual from the reach of the modern state. Underpinned by a techno-libertarian ethos of personal liberty and freedom of information, early hackers prized decentralized systems as powerful political commitments whose structures would go on to reshape society in a similarly "decentralized" image. The traditional hacker practices of creatively breaking and repurposing existing systems in subversive ways were thus extended to the creation of new systems, which might then "hack" society into a new shape.

As the hacker subculture spilled out from research departments to the growing hobbyist computing movement and the underground forums of the internet's "demimonde," it developed a far wider cultural relevance of its own. If the hacker's fear was of a dystopian digital future dominated by high-tech corporate and military power, then the hacker herself was an

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

individual whose technical prowess would allow her to both surf the waves of technical power and disrupt them from below. These ideas flourished in depictions of hackers from science fiction: Brunner's *Shockwave Rider*, Gibson's *Neuromancer*, Scott's *Trouble and Her Friends*, the Wachowski sisters' *The Matrix*, and more recent books such as Thompson's *Rosewater*, to name a few.

The hacker is now a core cultural archetype of our societies. Hackers and hacking are often in the news and are regularly featured in media from action films to video games.[9] Accordingly, there is now substantial academic scholarship on real hacker subcultures, initially portrayed as male, introverted, and based around a narrow set of values. It is now more widely accepted that "hacking" happens in a truly diverse range of communities, often with very different goals and perspectives but that share a core commitment to technical curiosity and experimentation.[10]

The world of the hackers fragmented into a range of overlapping perspectives and cultures across the 1980s and 1990s. Coleman and Golub describe three central cultures of the wider hacker ethos: *crypto-freedom*, *free software*, and the *hacker underground*.[11] Although all steeped in essentially liberal values and hacker practices of creative engineering, each emphasizes a different facet of the hacker ethos, reflecting the tensions and discontinuities within liberal thought. Each of these three hacker worlds has retained an enormous influence over the politics of the internet, and each continues to this day to shape the Tor Project.

The first of these, crypto-freedom, is particularly important for this history, as its ideas would eventually form a core part of Tor's development and reason for existence. The crypto-freedom culture derives from the computer scientists and cryptographers who were developing the encryption technologies that grew up alongside the internet. Cryptography and codebreaking had historically been technologies of the state, but a new generation of academics, engineers, and researchers had begun to imbue them with a newly anti-authoritarian, utopian character. The ease with which new digital technologies could be created and distributed meant that those new technologies could far more easily be put in the hands of the people, and thus exist for the benefit of the public, not just the elite. One researcher in particular, David Chaum, the "godfather of the crypto movement," spent the late 1970s and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

much of the 1980s laying the foundations for many of the technologies circulating today, with early designs for digital cash and cryptocurrencies, electronic voting systems, anonymity networks (called *mixnets*) and several core cryptographic tools of the digital age.

For the self-named *cypherpunks* involved in this work, encryption technologies took on an explicitly political character: they could have a powerful impact beyond military use by underwriting a libertarian conception of privacy and autonomy of the individual, protecting the internet as a space for freedom and information, commerce and community.[12] This commitment to action (rather than political wrangling) was summarized in the motto: "cypherpunks write code." While they shared a utopian view of the internet with other hacker sensibilities, they believed that maintaining that utopia would require robust technical mechanisms for ensuring privacy, lest the internet become a dystopian tool of repressive control and surveillance. To the cypherpunks, this vision could be realized by the math of cryptosystems, formal proofs that could quantify in hard numbers the privacy properties of the systems they were building.[13]

Beyond the academic research community, a wider cypherpunk movement developed as an association of cryptographers, hackers, and privacy enthusiasts centered around the infamous *cypherpunks mailing list*.[14] This loose network of people, concentrated in the San Francisco Bay Area, would develop into a small but influential political movement. As the US government attempted to discipline the increasingly unruly early internet through arrests, technical controls, and repressive new laws, the cypherpunks saw themselves as the resistance. In addition to fighting in the courts and through advocacy, many resisted authoritarian control of the internet by making new systems, often in the form of anonymity networks and encryption technologies. Still others sought to break the architectures of control emerging around them, attempting to find cracks in existing systems and in the technologies through which the government was trying to manage and control the early internet. As no government or private company could be trusted with the power conferred by a single point of oversight, the technologies they built—for file storage, communication, and commerce—tended to revolve

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

around decentralized networks. For the cypherpunk movement, just like other hacker worlds, decentralization was a political value of its own.[15]

The second of these hacker worlds developed around the open source movement. Some of the hackers who had played a role in the internet's early years of development had begun to set up foundations and communities dedicated to developing software in a new way, one which would embody their techno-utopian values and hopes for the internet as a vehicle for social transformation. In reaction against "closed" and "proprietary" models of software development, in which source code is copyrighted and obfuscated to prevent unauthorized copying or changing, they envisioned a future internet in which code was the foundation of a radical democratization of the material underpinnings of social life.[16] By opening up source code to public scrutiny, they argued that as the internet became more central to everyday life, so too should it empower people to question and shape the ways in which the programs they depended on actually functioned.

This was underpinned by an ethic of radical participation, which held that not only should the source code be viewable to everyone, but the people who use it and others interested outside the academy and industry should be able to take part in its development.[17] The freedom to participate was held to be as important as freedom from surveillance, and as such there was a priority placed on the free and open sharing of ideas as well as the right to experiment with technology free from regulation.

Privacy was a rather different matter to these groups. They were more concerned with taking the radical new technologies of the internet out of private corporate control and opening them up to the public. For open source communities, a more private internet was as much about giving the public real power over the design of digital systems as it was about hiding what they were doing with them. As these organizations watched the tools and hobby projects they were building become vital infrastructure incorporated into internet systems across the world, they often struggled with the internal politics of their work, trying desperately to manage large communities of contributors who often had very different ideas about the directions they should take. The resulting conflicts meant that some parts of the open

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

source culture began to develop a dislike for overt political wrangles, preferring instead to focus on the technology.

As the 1980s progressed and hobbyists and computer enthusiasts increasingly gained access to networked computing, a burgeoning hacker underground developed.[18] During this time, a range of other computer networks, often set up by user communities, proliferated outside of the US government's ARPANET. Two of the most famous were Usenet, a community platform that operated as a series of discussion boards, and Bulletin Board Systems (BBSes), a set of homemade bulletin boards hosted on user computers that could be connected over telephone lines. These networks, built by the communities that used them rather than being handed down by a faceless company, developed a set of vibrant cultures of their own.[19] In many of these communities, the users—a mix of adults taking home their first personal computers from work and their kids experimenting late into the night—were realizing that the documents, files, music, and games that they were buying in the shops could be shared for free in digital networks.

In these hobbyist communities, a distinct hacker subculture began to arise, similarly concerned with technological experimentation, creativity, and anti-authoritarianism, but more interested in disrupting and subverting power than creating cryptographic tools or participating in an open software organization.[20] Steeped in these techno-libertarian ideals, and incubated online and through in-person meet-ups (which still exist today), this subculture grew into the "hacker underground." It was composed of a range of internet communities engaged in sometimes criminalized attempts to hack, repurpose, tinker with, and exploit computer systems for any of a number of reasons: out of curiosity, to establish a reputation, for personal gain, or for political purposes.[21] A substantial cultural life emerged from these communities, exemplified in many of the films and novels that deploy the figure of the hacker.[22] When criminologists and law enforcement talk about hackers, this is generally who they are referring to.

These three distinct hacker worlds have played crucial roles in the development of the internet. Cypherpunks have created encryption and anonymity technologies that are now fundamental to global finance and communication, as well as more contested privacy technologies such as Tor

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

and Bitcoin. Free software can be found as a component in almost all technical systems and provides the backbone for huge swathes of the internet (Tor itself is developed open-source and draws on many of the beliefs of the open source ethos). And the hacker underground has been a powerful force, allying with social and activist movements, becoming involved in more serious crime, and provoking (and resisting) a backlash of control from governments. Still more hackers who grew up in these communities have spilled out of the academy, free software communities, and the underground into the corporate world, where the ethic of internet-mediated disruption has upturned entire industries and led to the creation of entirely new power structures.

In the following years, the 1990s, the internet grew away from its roots as a military and scientific network into a more familiar commercialized form, open to businesses, everyday users, and global commerce. Though the internet had previously been largely managed by a technical and scientific elite, by the 1990s, it had become a space of capitalist exploitation of interest to businesses and corporations.[23] As the internet grew, the development and popularization of email, bulletin boards, and other such applications marked the beginnings and growth of a consumer market for internet-connected technologies. This then led to the military handing over custodianship of the internet to the National Science Foundation.

The dream of an internet open to everyday users and commerce was realized in the creation of the World Wide Web in 1991. On the web, users were able to explore networks through *websites* where text and multimedia content could be hosted. These websites were connected through hypertext *links* that created a semantic connection between different websites. The release of the Mosaic web browser in 1993 and early search engines began the expansion of the internet to an even wider audience.[24]

Behind the vision of a commercialized internet forming the basis of new global free markets in ideas, commerce, and communication is a school of thought called *neoliberalism*. The neoliberal vision of the world idealizes the dissolution of national and international barriers to free trade, free movement, and communication, with a vision of modernity synonymous with the spread of capitalist democracy and market freedom around the world.[25] It views the market as the true arbiter of democracy, bringing democratic force

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

to the provision of every public good, as the public "votes with its money." *Neoliberalism* sees markets—much like the internet itself—as a powerful cybernetic system for information exchange and self-regulation, maximizing efficiency and quality through competition. Hence, in this tradition, states should intervene minimally, if at all, in the operation of markets—setting the conditions rather than picking winners. This model is at least in theory deeply suspicious of direct attempts by states to govern from a centralized position.

In practice, this involves the delegation of traditionally public services (including maintaining order and other policing functions) to the private sector and free market competition. The irony of these *laissez faire* postures of the state within neoliberal government is that they traditionally entail the presence of extremely strong forms of state control in order to enforce and protect these free markets and keep them from going haywire.[26] Control becomes, therefore, a force enacted at a distance, with states "steering, not rowing" the boat.[27] This vision of the world has been roundly critiqued by a vast scholarship of political and social scientific thought (and by social movements and civil society groups) for its naivete toward (or calculated disregard for) the effects of such systems on the poorest in society, their tendency to concentrate wealth and power, their implication in neocolonial geopolitics, and the entrepreneurial, consumerist, individualized vision of the subject and the citizen that they create.

As the Cold War ended, many in the West heralded the "End of History," with neoliberal capitalism triumphing over Soviet communism as an unchallenged and eternal global order.[28] The internet and the World Wide Web grew up in the shadow of these ideas, which today seem laughable, and the governance regimes and shape of the internet that developed over the 1990s are reflective of this.[29]

This can be seen in much of the neoliberal discourse surrounding the internet in this period, which framed it not only as enabling free markets but, through a kind of technological determinism, embodying open and decentralized structures that inherently promoted democratic and free market capitalist forms of society.

> Liberty will be spread by cell phone and cable modem . . . We know how much the internet has changed America, and we are already an open society. Imagine

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> how much it could change China. . . . Now there's no question China has been trying to crack down on the Internet . . . Good luck. That's sort of like trying to nail Jell-O to the wall.
>
> President Bill Clinton, speaking in 2000, quoted in John Lanchester[30]

Again, the value of decentralization (or at least the fantasy of decentralization) rears its head, in this quote appearing painfully naive. Privacy here emerges as a form of US soft power, as a way to undermine governments like that of China, based around centralized state control and authoritarian surveillance. Many of the foundational policy papers and documents that led to the formation of core internet governance organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) were explicitly neoliberal in sensibility, imagining the internet as facilitating the proliferation of free markets and competition.[31] This extends both to the *purpose* of the internet, but also to how it is administered, largely delivered by private companies competing in an ostensibly free market. However, the ways in which the internet and online power have developed in recent decades reveal the tensions within neoliberal visions of society and how easily these free and decentralized structures can be repurposed for control and repression.

The commercialized, global internet soon began to present problems for the very nation-states that had championed its early development. If the internet were to support business, commerce, and communication in global free markets, it would require robust mechanisms to protect traffic from eavesdroppers.[32] No corporation trading internationally would allow their sensitive communications to be vulnerable to their rivals, or visible to the government of every country in which they did business. As the network spread to these new users, the cryptographic technologies invented by the cypherpunks and academic researchers took on a new importance outside their traditional military applications.

For much of the 1980s and 1990s, cryptographic protocols remained categorized by the United States as munitions for export purposes, a hangover from the period following World War II, when such technologies were nearly exclusively in the hands of the military and the US was loath to allow other nations to use them.[33] With the invention of the World Wide Web in 1989, its release to the public in 1991, and the release of the Mosaic web

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

browser in 1993, internet use began to spread beyond businesses, the military, academics and hobbyists, and a burgeoning consumer market emerged. Encryption technologies, suddenly vital for business and citizen use of the internet, posed a number of issues for law enforcement and the military as they fell into the hands of the public.[34]

In particular, law enforcement, intelligence, and government agencies in the United States viewed encryption as a direct threat to the ability of the criminal justice system to maintain order, protect national security, and investigate crime. The creation of social spaces and forms of communication that could not be surveilled posed what appeared to many policymakers an unacceptable obstacle to the practice of intelligence gathering.[35]

This resulted in a range of attempts at policymaking in order to permit the use of encryption for security and the protection of consumer and business privacy, but also to allow law enforcement agencies and intelligence services access to communications and data *in extremis*. This marked the beginning of the *Crypto Wars*, a protracted series of attempts by governments (especially in the US) to compromise and weaken encryption, a fight that continues to this day.[36] These proposals ranged from physical compromise of machines through technologies like the Clipper chip (which would allow authorities access to encryption keys), to limiting the strength of encryption allowed for sale to consumers, to "backdooring" encryption technologies (by which secret weaknesses would be built in that could be exploited.)[37]

As these efforts ramped up over the 1990s, they galvanized substantial resistance from within both the technical and academic communities and from civil society groups. In particular, they led to a call-to-action from the cypherpunks, who sought to resist across a variety of domains. In addition to policy engagement, lobbying, and legal action, they continued to develop and popularize the use of encryption technologies.[38] They also used more creative methods of resistance, including eye-catching stunts, such as undermining the export regulations on strong cryptography by having the code of encryption programs printed on T-shirts, which would hence allow them to fall under constitutional protections for speech and expression.[39] It is at this point, in the mid-1990s and at the height of the Crypto Wars, that Tor's history truly begins—with the Onion Routing Project.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

3 TOR'S STRANGE BEGINNINGS

Tor's story began in earnest against the backdrop of the Crypto Wars of the mid-1990s. As with so many of the internet's origin stories, it began not in the wild, open horizons of computer networks, but in a tight physical space: an office of the US Naval Research Laboratory (NRL).

Down the hall at the Laboratory, satellites and radar dishes hung suspended in enormous voids, giant black pyramids bristled from the walls of vast anechoic testing chambers, and robot arms flexed in dark flooded pools, being poked and prodded by scuba divers armed with sensors. But the foundations of Tor were laid in a much more prosaic setting—a shared computer lab.

Three military researchers—David Goldschlag and Mike Reed, who shared an office in the NRL's Washington, DC campus, along with Paul Syverson (who regularly carpooled with Goldschlag)—had been discussing a foundational aspect of the internet infrastructure: the link between the identity of individuals using the internet and the protocols used by internet traffic to arrive at a destination. While some of their research was commissioned directly by the US military—to solve a clear problem in need of a solution—much of it was more open-ended, with the aim to stay ahead of future developments. As a result, these kinds of conversations—in the car, the coffee room, or walking the corridors—were not unusual, and were crucial to their wider body of work.

The rise of the new, commercial internet presented challenges for military users, as these global systems were vital for communications but difficult to secure. For these same reasons, however, it was of interest to the communications security researchers of the NRL. The internet's traffic

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

routing systems and protocols are reliant on addressing metadata, equivalent to the *to* and *from* addresses on an envelope. Much as the address of the recipient is crucial for the delivery of a piece of mail, so are these metadata fundamental to the internet's design and necessarily visible to the infrastructure providers who run its networks. The researchers wanted to find a way to do the seemingly impossible—to give the military the benefits of a global, high-speed communications network without exposing them the vulnerabilities of the metadata that the network relied on to operate. Their signals would need to navigate the internet while their origin and destination remained invisible to the people who ran the infrastructure itself.

The US Navy might, at first glance, seem to be an odd home for the development of cutting-edge internet technologies, but securing communications has been a long-standing priority of naval forces around the world. Ships and submarines at sea need to continuously transmit and establish their positions, maneuvers, and actions remotely. Disguising these signals and preventing them from being intercepted or read is both extremely difficult and an absolute necessity (for reasons familiar to anyone who's ever played the board game *Battleship*). As a result, secure communications research has long had a home in the US Navy—along with core aspects of the US space program and other seemingly innocuous avenues of study.

Much as with the development of the internet's traffic routing model itself, a decentralized model for *identity* and *traceability* has notable security and resilience benefits for military uses. The centralization of the internet around internet service providers (ISPs) and the inherent traceability of communications pose the same problems for the military as for human rights activists and privacy-conscious citizens: the capacity for a government or nation-state to observe the internet within its own borders.[1]

This design—centralized enough to provide clear "control points," but not enough to produce single points of failure—works well for the US government's domestic interests, as it allows the state to establish itself at key control points and surveil user traffic. However the spread of the internet around the world has also given non-US governments this power over their own domestic communication networks.[2] This means that US intelligence and military personnel abroad who want to make contact with their

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

handlers in the United States or communicate with their base of operations are vulnerable to surveillance if they do so using the internet. Whenever the Navy utilized cryptosystems and communication networks that linked up to the internet, substantial amounts of valuable additional information were exposed to the people who ran the infrastructure.

Although encryption technologies protect the *content* of messages, the administrative information that these messages use to route themselves to their destination can itself be extremely revealing.[3] For example, if a CIA spy is in a foreign nation and sends a message over the internet back to the CIA's home servers, ISPs in that foreign nation can observe that the message was sent and infer the spy's affiliation.

Protecting this routing information from surveillance is extremely difficult, as the signals need to be able to travel through the internet to their destination, and so at least some of this information needs to be exposed. Even if the US government were to run its own network of servers that could hide users' traffic, in practice, this would mean that the authorities could observe someone connecting to, for example, the CIA's secret anonymization network, and hence trigger even more suspicion.[4]

There existed a clear problem: how to keep internet traffic between the US and other nations secret, not only in content, but also in origin and destination. The three NRL researchers sought to solve it.

In these early days of the internet, the potential risks that a global, widely used, and comprehensively surveilled communications system might pose to military users were still largely hypothetical. Funding for speculative research—trying to solve problems that no one had yet realized were problems—generally was not prioritized in military budgets. Although the NRL scientists were tasked with this kind of speculative research, they were not given free rein to do whatever they pleased. Instead, they had to pitch research ideas to internal funders to make a case for their future potential. To sell the idea of metadata-secure communication to their bosses, Goldschlag, Reed, and Syverson used an example that had been circulating in the press: the Pentagon Pizza Channel.

Following Operation Desert Storm, the US military's ground invasion of Iraq in 1991, a (possibly real, possibly apocryphal) story began circulating

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

on late-night talk shows. As the story went, a journalist had noticed a massive spike in pizza deliveries to the headquarters of the US Department of Defense in the Pentagon building the night before the unannounced invasion. From this, the journalist deduced that there were hundreds of Pentagon employees working late, and hence, that the invasion must be imminent.

To the NRL researchers, this provided a compelling example of how revealing metadata alone can be.

> And so we said—no one's doing this now, but imagine if in the future, you could order a pizza over the web! We said, an adversary could just, you know, watch the orders come into the local Pizza Hut or Dominos, and they wouldn't have to hang around outside the Pentagon, they could just watch the network.
>
> Tor developer

As more of social, political, and economic life moved online (a process only in its infancy in the mid-1990s), according to the theory, more of these "side-channels" would be revealed by the communications metadata produced by everyday activities. To the security agencies that controlled their country's domestic internet infrastructure, these metadata would be rich seams for analysis where signals of all kinds of secret activity might be spotted. This prescient warning convinced the NRL funders of the utility of researching mechanisms for metadata protection, and so the Onion Routing Project was born.

Work on the onion routing design began in earnest in 1995. Anonymity—or, more specifically, the separation of communications metadata from identity—had long been one of the "hard problems" of the internet. Unbeknownst to the three NRL researchers, a cryptographer and engineer named David Chaum had attempted to solve a similar set of problems in the 1980s through the development of *mixnets*, networks of servers that routed signals around, holding them at each stage to add delays, and then releasing them in a random order to "mix" the signals up. This meant that observers of the network would have great difficulty in untangling who was who in a "crowd" of users.[5]

Although many at the time speculated that onion routing was a development of mixnets, in fact, it was initially developed separately, more or less without reference to Chaum's design. What these two systems *do* share is

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

their use of the extensibility of the internet. Although the internet's control points and protocols "baked in" the use of metadata, the capacity of the internet to support higher-order infrastructures meant that a network could be built on top of the internet, in which these signals could be mixed and re-routed, with information being distributed around in such a way that no single part of the network (or observer) could identify its users.

Much of the early work on onion routing involved developing this core system design in theoretical terms and identifying the key issues that such a design might need to solve in practice. Onion routing has undergone many changes and refinements over the years, but the basic principle has remained the same. The routing information that packets of internet traffic use to navigate the internet is first encrypted, hidden under three layers of encryption like a Russian doll. It is from these layers that onion routing gets its name. This "onion" of routing information is then sent into a network of onion routers: servers, or *relays*, located around the world that bounce the traffic around and between themselves. Each of these relays decrypts a layer of encryption to reveal the address of the next server in the network, until the final server reveals the destination of the traffic and makes a connection to the target web service.[6]

This process serves to separate the information used to route signals from the identity of the user. Each relay involved in carrying the signal only has access to the previous and following steps in this chain: the first relay knows the identity of the person entering the network, but not where they are going, the middle relays only know the identity of other relays within the network, and the exit relay knows only the final destination, but not the user who made the request. This means that no single part of the infrastructure knows both the identity of the sender and the identity of the recipient, and so no part of the infrastructure can be used as a control point. If these servers can be set up in different countries around the world, this means that an adversary would have to have a global view of all internet traffic in order to deanonymize the users. This early work led to the publication of a design paper for onion routing at the First Information Hiding Workshop in 1996.[7]

This technical design has immediate social consequences, which were apparent to the NRL designers from the early stages. First, the infrastructure

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

could not be run by the US Navy, for if this were the case, then only people who trusted the US Navy would use it. In an onion routing design, anonymity is produced by the size of the crowd—the more people using the system, the more privacy it provides.

> But if we're the only ones running the system, then the only people you're going to get is the people who are inclined to trust us . . . So, you need to let mutually mistrusting people run different parts of the infrastructure. And that also underscores its security, because if they're running it, and it's run by different entities, which are perhaps, you know, might be reputable, but are still not ones that you would expect to fully co-operate if somebody wanted to pull this apart.
>
> Tor core developer

There are other implications, as well. For a CIA agent to use Tor without suspicion in non-US nations, for example, there would need to be plenty of citizens in these nations using Tor for everyday internet browsing. Similarly, if the only users in a particular country are whistleblowers, civil rights activists and protesters, the government may well simply arrest anyone connecting to your anonymity network. As a result, an onion routing system had to be open to as wide a range of users and maintainers as possible, so that the mere fact that someone was using the system wouldn't reveal anything about their identity or their affiliations.

This philosophy, of a system open to the general public, in which small numbers of high-risk users could hide in cover traffic from more everyday users, underpins what became the onion routing paradigm, the predecessor to Tor.

> When I first said it, I thought I was being facetious, but in hindsight I think it was a reasonable thing . . . Well, you know, the technology's cool and it's nice to make something that's actually going to be useful and help people. But one of the really nice things about it is that you build something which by its very nature takes people who think they ought not to trust each other and work together at all, and forces them to collaborate in order to get the results that you want. And I just like the idea that you are forcing people who thought that they should never work with these people to do so.
>
> Tor developer

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

This requirement of widespread adoption, which would have the consequence of making the internet as a whole a more private space for its users, meant that the NRL team needed to sell online privacy—and the onion routing network—to the general public. In this, they shared interests with a range of groups that might traditionally be opposed to the US military establishment. Most importantly, the countercultural cypherpunks—the loose association of academics, security researchers, technologists, and privacy activists with whom the US government was battling over encryption—proved to be unlikely allies in selling the military system to a wider audience.

Aware of the need for mass adoption, the NRL researchers reached out to the cypherpunks, who were early adopters (and often designers) of privacy and anonymity technologies. A number of cypherpunks were invited onto the NRL's onion routing mailing list—a shared space to discuss designs, theories, and approaches to developing something that could have mass appeal. These mailing lists (and the subsequent mailing lists of the Tor Project) are still available openly in the Tor archives, and through these it is possible to read the two groups' attempts to negotiate between their cultures, along with many of the trademark in-jokes, technical humor, and low-stakes abrasiveness at the beloved shared heart of hacker culture.

These conversations also offer a glimpse into the culture of the Naval Research Laboratory, a culture that shares little with stereotypes of military life. Far from the crewcut jockishness that might come to mind when picturing a military base, the NRL culture was firmly rooted in the military-academic world familiar to many of the MIT scientists and hackers of the 1950s and 1960s. The NRL scientists' love of complex technical humor, sympathy for the anti-authoritarian and countercultural, and willingness to form unlikely alliances continued the legacy of these early hackers.

In these early stages of cooperation, some of the more fringe elements of the cypherpunks were deeply skeptical of the US Navy's desire to cooperate with them, much to the chagrin of the NRL:

> We are researchers. That is our job description. That is what we get paid to do. There are more PhD's walking around this base than some college campuses. We publish constantly in academic circles, we attend conferences, we participate in the larger academic world. Please do not assume that since we work for

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the government that we are uninformed, undereducated, GAK-loving idiots. What we lack is the practical experience in this area—most of what we do is theory, theory, theory . . . very little applied (at least in the computer security area). Thus the prototype where we've already learned a great deal about where the theoretical models break down in the real world. Thus all the discussions with people running other MIX variants in the world (both in research labs and actually out there on the Internet). Thus the need for a wider participation and the push for a general RFC that can be accepted by the whole Internet community. Please don't view this as an "us vs. them" environment . . . we want the same level (and possibly even higher level) of security that you want out of this system . . . help us do that. Sorry for the venting, but I've received one [too] many emails in the last two weeks from very uninformed people that have just rubbed me the wrong way.

NRL researcher, NRL onions mailing list, 1997

Despite this early skepticism, a critical mass of cypherpunks (many of whom were themselves researchers and engineers) saw the potential for collaboration. One was clear in their response:

The mere fact that you are working on Onion Routers proves that you have a clue and are none of the things that you seem I am assuming. I assure you, I am not assuming any of the traits you mention.

Which is exactly the reason why I am talking with you, published your URL to the relevant mailing lists, and convinced people I knew to be knowledg[e]able about this topic to subscribe to this list.

This is not an "us vs. them" for any person on the list that I know. And I probably know most, if not all subscribers (other than the ones from NRL, whom I first met at FC'97).

Most of the non-NRL subscribers on this list are, or have been, subscribers to the Cypherpunks mailing list. The overriding goal was to secure the communications infrastructure and achieve privacy by preventing the adversary from gaining information about an individual or corporation by being able to read or traffic analyze the communications. Classical COMSEC.

Cypherpunk, NRL onions mailing list, 1997

As they worked together on developing the core technical design of onion routing, this meeting of worlds flourished:

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> The old Cypherpunks and the US Navy are facing the same problem and are therefore looking at similar solutions. You need broad public use of the system to provide you with cover traffic and we want to see such a system deployed to provide the citizens with privacy. We are allies, not enemies.
>
> It is in this spirit of cooperation that we are pointing out issues with your design that some of us believe require fixing before the system can achieve our common goal. We all want to see the best design possible to be deployed, because we all know that no other design will ever achieve the broad penetration that we seek. Let's all work together on making that design a reality.
>
> Cypherpunk, NRL onions mailing list, 1997

After corresponding via email, the NRL researchers met several members of the cypherpunk community in person at the Information Hiding Workshop in Oakland in 1997. The NRL developers discussed the possibility of collaboration, to together figure out what kind of system the military could create that would actually be used by the privacy-conscious general public. This culminated in another physical event that crystallized the developing collaboration: the Onion Dinner, a meeting during the Information Hiding Workshop (including a range of onion-themed food) in which the potential goals and futures of onion routing were discussed in depth.[8] Raph Levien, a cypherpunk living in the Bay Area, invited other members of the list, who were planning to meet together for the first time, to his house down the road from the conference venue.

> As promised, finally an invitation. I think it would be great if the onion routing people could get together with a group of cypherpunks who have put some thought into this problem. Since the onion routing people will be in the Bay Area for Oakland, and since most of the relevant cypherpunks live here . . . I'd like to organize a dinner at my apartment sometime during the Oakland conference . . . I'm willing to try some onion recipes. I think this would really give us the chance to talk seriously about network anonymity, and get to know each other better.
>
> Cypherpunk, NRL onions mailing list, 1997

Over vegetarian lasagna, salad, and (what else?) roasted onions, they discussed the technical possibilities and paradigms that might underpin a

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

mass-use anonymity system. As they did, they also talked through broader values and motivations that might unite their strange, hybrid community.

> I think it is clear that we all have the same goal: to provide a privacy protecting infrastructure for near real-time net connections. Sure, some people out there will flame you because they are convinced that it all is a giant plot by NSA/NRL/AT&T, undoubtedly organized by the Illuminati, the Elders of Zion, and of course the Trilateral Commission. The people on this list do not fall into this category. You'll just have to ignore the naysayers, though some of them may have some valid technical advice to contribute.
>
> The various systems proposed all have their advantages and drawbacks. There is good reason to continue parallel development.
>
> None of us really has any hard numbers to back up their assumptions. I believe further development would benefit greatly from subjecting the systems to information theoretic/signal analysis. For example, it seems to me that we are all just guessing if additional cover traffic has to be added or not. My experience with remailers suggest it does, others disagree. But nobody has actually done the math to prove or disprove either claim.
>
> That's all for now. Time to go to bed :-)
>
> Cypherpunk, NRL onions mailing list, 1997

Several of the cypherpunks would go on to play a long-term role in the efforts to create Tor. While the development remained largely led by the NRL scientists in the 1990s, these cypherpunks played a vital role in reviewing and shaping the direction these efforts took. The birth of onion routing therefore represents a confluence between two distinct, but overlapping, visions of the internet: the interests of the military, and those of the cypherpunks.[9]

The ways in which these two worlds make sense of privacy are not in fact that different. Both the cryptographers working as US military researchers and those of the cypherpunks had a deep technical understanding of computer systems, and were attempting to make changes to the structures of these systems in order to undermine the ability of nation-states to exert centralized control over the internet infrastructure. In other words, both groups wanted privacy from surveillance. One, however, wanted privacy *from* the US government, and one wanted privacy *for* the US government.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

This tension between freedom and control was also already evident within the US government alone. While one arm of the US government was trying to clamp down on encryption, another was developing a technology which would give strong anonymity protections to large parts of the world. This tension would only become more evident as onion routing continued to grow.

Even at this stage, the cypherpunks and NRL designers were moving beyond abstract designs. Over the next few years, they would set up test networks, generate metrics, measure speeds, and try out new potential attacks against the system. The design was also evolving, as they experimented with different kinds of padding, adding (and then removing) mixing of the traffic at the nodes, and trying different numbers of hops through the network. The core issues and controversies that would define the early development of Tor were crystallizing. Some of these related to design issues (how many hops the traffic would take between nodes before exiting the network, or whether to add fake "padding" traffic to confuse attackers) and others concerned the social organization and rules of the Tor community (would they allow anyone to set up their own node? And what kinds of control would node operators be able to exert over the infrastructure?).

Other groups began using code and ideas spilling out from onion routing. The need for the network to be trusted by people who didn't trust the US Navy meant that the group was making much of their discussions, development ideas, and source code free and open, releasing it directly to the public and academics to scour for hidden traps and backdoors. Many other groups—some of whom had been developing their own mixnets, anonymous mailing, and hosting systems—began experimenting with, borrowing ideas from, and contributing to onion routing. It is from these early communities that Tor would assemble its first coalition of developers and maintainers.

Many of the issues emerging at this stage, as the onion routing design was beginning to take shape and be tested over the mid- and late 1990s, related to finding a balance between adding established design features on the one hand, which would add security on paper (but which almost all slowed the system, reducing the potential pool of users and relay operators), and maintaining mass usability and public adoption of the system on the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

other. Onion routing had fierce competition, particularly in the form of the mixnet design. Mixnets, as the name suggests, add traffic mixing to a routing network, with signals being held, delayed, and reshuffled at the nodes in order to confuse those watching the network and make it much harder to deanonymize the traffic. This provides a defense against attacks that involve timing, counting, and tracing the signals traveling the network, or spotting patterns (for example, if someone always uses the network at the same time). Why—the proponents of mixnets asked—would anyone use this less secure technology being developed by the onion routing community?

Crucially, the additional protection added by mixnets comes at a cost—it slows the system down. This might be acceptable if your main application is email, but as the commercial web developed, people wanted to use it for much faster browsing and communication. In the late 1990s, very few people were using any of the big mixnet networks, and so any adversary trying to deanonymize them only had to do so in a crowd of a few hundred users. Onion routing, whose values and core design were increasingly based around usability and mass uptake, framed these issues in terms of greater adoption—a more usable system was a more secure system, as it would have a larger and more diverse "crowd" to get lost in. This was often formalized in the dictum "anonymity loves company."[10]

Throughout the discussions on the onion routing mailing list, privacy was rarely mentioned. Instead, it was left implicit as a cypherpunk value. Instead of privacy, these conversations were about *anonymity*, one way of recasting privacy politics in technical language. In this, however, privacy was beginning to be associated with the ideas of network structures and decentralization. Already, the onion routing engineers and cypherpunks were beginning to distinguish themselves from many of the values and practices associated with cryptographers. Cryptography tends to inhabit the world of math and formal proofs, with harder security measures theoretically provable as conferring better security. However, as the cryptographers and cypherpunks were finding, the math wasn't enough on its own. At many points, design features that might appear to provide mathematically sounder security failed in the "real world" as they became too onerous for users.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Onion routing responds to the usability end of this argument—the bigger the crowd of users, the better security it provides. Because of this, the technical design was inherently bound up with a vision of privacy as usable, everyday, and embedded in society.

Observing these two worlds—the military academics and the cypherpunks—interacting, through sharing test results, theoretical discussions, phone calls, emails, and eating the occasional roasted onion, we see the beginnings of a new privacy world. The technical heart of onion routing, in which a large and diverse group of everyday users drawn from the general public creates cover traffic for a small number of users who need very high security protections, provides the perfect space for the values of these two distinct cultures to come together. The clever thing about onion routing is that it makes these two radically different versions of privacy rely on one another. Onion routing forms a conduit between these worlds, binding them together and making the cypherpunk's everyday, radical, decentralized vision of privacy and the high-security traffic protection desired by the military mutually dependent.

At this early stage, the idea of privacy as written into the structures of internet power and control was clear in the emerging technical design. As the cypherpunks began to make these connections back to their military-academic roots from the early days of the internet, they brought with them their commitment to decentralization, radical social change, and their desire to use the internet and its technologies to shape society for the better. The NRL brought a connection to the US security establishment, and with it, funding, expertise, and an impetus to make this project a reality.

When the two groups begin to build a real system to be pushed out into the world, we will eventually see this collaboration deepen, and their two disparate worlds finally join in the birth of a new social world—of the Tor engineers.

This meeting of worlds was not always smooth, and as the Tor engineer world was forming, political conflicts spilled out of the evolving technical design. The first post archived on the onion routing mailing list in 1997 sets the tone for much of the next twenty years of Tor development:

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> [Cypherpunk] Besides possible attacks, I'm also concerned about possible abuses of anonymous routing systems. Have you thought about how to prevent things like hackers breaking into computer systems while maintaining anonymity with the Onion Routers?
>
> [Onion routing developer] That is a political question, and to date, we have tried to only deal with the technological issues instead of the political ones. As soon as we start dealing with political issues, this thing will fall apart.
>
> Conversation on NRL onions mailing list, 1997

As we will see, this broke down quickly on contact with the real world, but the suspension of politics (and the transfer of some political discussions into the safer language of technical system design) would prove important for many years to come. First though, everyone involved needed to take these ideas, models, theories, and paradigms and turn them into a real system—Tor.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

4 DESIGNING THE ONION

The internet was an odd place in the early 2000s, especially if you were an IT engineer with radical ambitions. With the turn of the century, the utopian dreams of the internet were already giving way to a rather bleaker future. The dream of a globalized society underpinned by an endlessly expanding internet was shaken first by the dot-com bubble bursting, when a vast supply of cheap money and enthusiasm for new technology flooded into markets, resulting in the massive overvaluation of companies with flashy branding but no real product, and then its subsequent painful return to Earth. The recession accompanying this crash in the early 2000s, and further collapse and consolidation of the tech market around a few large firms, heralded the beginning of a more sober and pessimistic era of internet expansion (at least until the social media boom at the tail end of the decade).[1]

The backdrop to the next chapter of Tor, when the ideas of onion routing were being turned into a real system, was however defined above all by the September 11 attacks and their aftermath, the West's Global War on Terror. This reshaped the structures of power traced by the growing internet, which to the military and intelligence communities seemed to morph almost overnight into a vast, chaotic sea of communications intelligence vital for preventing further attacks on the United States. It became clear to US policymakers that as in addition to a technology of free information and markets, the internet was also a source of intelligence—an opportunity to understand and exert influence on an increasingly chaotic world.

In trying to tame the internet, the West's security services would over the next decade redraw its lines of power, building covert data collections

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

into the bedrock of its infrastructure, establishing international intelligence-sharing alliances, and collaborating with the vast corporations that managed and created online space.[2] Although rarely made explicit, the idea of the internet as an active battleground of global power hung above the early days of Tor and was written through the design documents, arguments, and cultures of its formative moments.

Over the late 1990s and early 2000s, a loose network of technological resistance projects was growing, drawing on onion routing and similar distributed systems. These projects sought to repurpose the internet in different ways to break up corporate and government power. Many sprang up out of the same people and values as the illicit file-sharing scene of the late 1980s and the 1990s, with the same lo-fi, high-tech aesthetics. They mostly resembled academic hobby projects, start-ups, and small enthusiast communities, though some achieved genuine mainstream success. Anonymous remailing systems, used to provide secure email to a few dozen people, jostled with file-sharing experiments in which millions of science fiction nerds and music enthusiasts traded illicit copies of films, albums, and video games.

If not always in their branding, these projects were at heart motivated as much by a practical interest in seeing what the newly popular technologies of the internet could do as by political values of techno-resistance.[3] They would continue to spring up like mushrooms over the next few years, with some achieving widespread use and notoriety. This was particularly the case for file-sharing services, which promised an internet future synonymous with free music and video. Many children of the 1990s in the United States and United Kingdom remember adolescent experimentation with Napster, BitTorrent, and LimeWire, but few signed up for more esoteric projects like Mixminion, GNUtella, or Zero-Knowledge Systems' Freedom Network.

Many of these projects can trace their lineage back to a seminal paper by a security researcher named Ross Anderson. This paper, published in 1996, set out a vision for a decentralized system of file storage called The Eternity Service, in which digital files would be split into chunks and smeared across a network of storage servers around the world. [4] In this system, there would be enough duplication to ensure that even if half the network were taken down, the files could still be reassembled and downloaded.[5]

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Anderson's paper helped set the technical agenda for decentralized and anonymous visions of the internet. Many of the "resistance tech" projects of the late 1990s would coalesce around designs that explicitly decentralized control around the user network, with central authorities playing mainly a coordinating function. Unlike open-source products, the wider user bases of these products weren't expected to take a deep interest in how they worked or hack on it themselves, but instead only to take part in a community-at-a-distance mediated by the technological design. Well-known services like Napster (launched in 1999) and BitTorrent (launched in 2001) relied on a social model—you download the files you want and then upload (or "seed") tiny parts of them to other users (lest you be condemned as a "leecher" who doesn't contribute).[6]

Along with the file-sharers, this period saw a range of geekier projects focused on providing anonymity to internet users (whose names, ironically, are mostly lost to history): Mixminion, FreeNet, Zero-Knowledge Systems' Freedom Network (a commercial anonymity network run for profit), and the Crowds system run by AT&T's research division, to name a few.[7] Many of these projects—constructed by hobbyists, researchers, start-ups, and activists—were built around implementations of onion routing, mixnets, or similar designs. Instead of the immediate and visible personal benefits of participating in file-sharing—receiving cracked copies of a game yourself, or getting a fuzzy feeling as you helped someone else download a copy of the video game *Deus Ex* or dodgier files like *all_along_the_watchtower_Linkin_Park.exe*—the benefits provided by these anonymity services were a little more intangible. You can't see or feel online state surveillance, so you can't really see or feel its absence either. Instead, participation in these projects was generally driven by a mix of abstract (but strongly held) beliefs in freedom, privacy, and human rights, along with a hackery love of intricate tech solutions for their own sake—in other words, the realm of the cypherpunks. But cypherpunks alone couldn't sustain a mass-use system, and these systems were rarely adopted by enough users to form a crowd large enough to frustrate a motivated attacker.

It is at this point that two of the major characters in Tor's history appear: Roger Dingledine and Nick Mathewson. Dingledine and Mathewson, both

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

computer scientists pursuing master's degrees at MIT, were living in the same dormitory and had become fast friends, bonding over a shared interest in computer security and together embarking on failed attempts to make an online "Multi-User Dungeon" multiplayer video game and a user-friendly distribution of the Linux operating system. Both had an interest in the wider politics of software projects; alongside their lectures in math and software theory, they were reading radical authors, from Mahatma Gandhi and Dr. Martin Luther King Jr. to more cypherpunk works by technologists like Bruce Schneier.

Dingledine, much as he does now, presented a rather unassuming image to the world: a tall man with glasses and a ponytail, inevitably sporting sideburns and a T-shirt with the logo of a hacker project, he appears every inch the 1990s computer devotee. As a young, enthusiastic graduate student at MIT, Dingledine had been a living synthesis of the cypherpunk and military-academic worlds, having been sucked into the anonymity and crypto-hacking scene along with more "legitimate"' employment, including working on his university's own network security team and a summer internship at the US government's National Security Agency.

Inspired in part by the "beautiful world" conjured by Ross Anderson's Eternity Service, Dingledine was involved in a range of smaller, more niche anonymity projects. We can get a snapshot, at the very least, of the values motivating Dingledine from his master's thesis at MIT. Much like the Eternity Service paper and other crypto-freedom writing of the time, it blends discussions of law, policy, and the moral, social and, philosophical value of anonymity with technical detail on the design of anonymity systems. It proposed a vision of the internet that would become the expansive manifesto of the Free Haven Project—effectively a list of technical issues that they wanted to "fix" in the internet infrastructure to bake in its utopian ideas.[8]

It seems rather odd now, in the era of cloud computing, but Dingledine's utopian vision of the internet was built around the idea of file storage. The Free Haven Project was, at least partly, Dingledine's attempt to design a real-life Eternity Service. The Free Haven Project wanted an internet that could speak truth to power—one that looked a little bit like BitTorrent or Napster, but with the values (and commitment to anonymity) of something like Wikileaks. Free Haven would be used to anonymously host files that

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

couldn't be taken down, and which were spread in duplicated chunks across a network of servers—much like Anderson's Eternity Service. The Free Haven Project saw anonymous, censorship-resistant file storage as essential to many of the internet's most radical and liberating potential futures—hosting more than just bootleg Paul McCartney songs, but also rebel newspapers, leaked CIA documents, evidence of corporate corruption, and anything else that the powerful didn't want you to share.

To achieve this vision, they would need to fix a lot of what was broken about how the internet worked. And at its heart, one of the core design problems underwriting all the others was the issue of anonymity—how to access Free Haven without being spied on or blocked. Fortunately, this part of the problem had an actual solution, emerging at the NRL in the form of onion routing. Dingledine, and later Mathewson and a range of others, would spend the next twenty years working on this first step to realizing their dream of a possible future internet.

This dream initially found a home in a project they called Mixminion—an attempt to build a new generation of mixnet remailer (following in the footsteps of the earlier Mixmaster project) into a basis for Free Haven.[9] This brought Dingledine and Mathewson into contact with the wider remailer and anonymity community and the plethora of systems being developed—a chaotic mess of instant messaging channels and mailing lists, some of which were full of spam and roiling, toxic flame wars. But despite this, the two researchers quickly immersed themselves in the wider "anonymity" community—a loose group that would become vital in shaping how they understood what it meant to make privacy a reality in software.

In particular, it was becoming clear to them that engaging with the debates in their academic studies and the loudmouths on the cypherpunk mailing lists was very different from dealing with the practicalities of writing code and developing systems that people could actually use. As Mathewson began developing the software base for Mixminion—itself a fun challenge as he built up his chops in software engineering—the corporate attacks on file-sharers provided an ominous backdrop, as their efforts focused increasingly on undermining online anonymity (not just encryption) through legal and technical means.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Amid this soup of technical resistance projects, and while state and corporate powers were mobilizing around choke points in the internet infrastructure, work was beginning at the NRL on developing the onion routing idea into a real, deployable system. Instead of partnerships between bedroom developers and moonlighting tech consultants, the loose alliance between the team at the NRL and the cypherpunks looked far more professional—these were, after all, people with mainstream legitimacy, resources, and technical power at their disposal. The space around issues of decentralization and anonymity was becoming denser and more networked than ever as the 1990s became the twenty-first century. Many of the key players in competing projects and communities were increasingly moving in the same circles, finding one another at the same conferences and workshops and fighting against the same issues related to corporate and state power. Many even had the same name (an indicator of the lack of diversity of the crypto field at the time), causing Dingledine to remark, in his thesis, on an "Ian conspiracy" of five key Ians in the field:

> Ian Brown (of the cypherspace datahaven design), Ian Clarke (of FreeNet), Ian Goldberg (of Zero Knowledge), Ian Marsh (of Jetfile), and Ian Hall-Beyer (of Gnutella) . . . why are the leaders of all these projects called Ian?
>
> Roger Dingledine, master's dissertation[10]

Later, of course, Tor would come to the attention of a rather different "Five Is." All this momentum coalesced in in July of 2000, in what would become the Privacy Enhancing Technologies Symposium (then operating as the Workshop on Design Issues in Anonymity and Unobservability). This workshop, held at the International Computer Science Institute in Berkeley, California, sought to bring together a range of people working on anonymity networks and decentralized file storage. Many of the bigger projects in this space were represented at the workshop, including Zero-Knowledge Systems (whose Freedom Network provided a paid version of onion routing), researchers working on Mixnets like Freenet and Free Haven, and the onion routing team from the NRL.

Paul Syverson and the team at the NRL had been continuing to develop their "original" model of onion routing. Enlisting Jim Proto, Lora Kassab, and Jeremy Barrett (part of a growing number of fellow onion routing enthusiasts

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

at the NRL), they had coded an implementation of onion routing and were subjecting it to a range of tests—simulating a small five-node network and allowing people to use it. But the project had reached a crossroads—they had only a small amount of grant time and money remaining, and the code they had wasn't even close to widely deployable. A regular on the crypto circuit, Syverson presented the team's work at the Berkeley workshop, discussing a paper on the current state of onion routing and their best analysis of how secure it might be. Presenting in the session right before Syverson, only a month after submitting his master's thesis, was Dingledine, who gave an overview of the Free Haven Project with some of his collaborators.

During one of the breaks at the conference in Berkeley, Syverson approached Dingledine, picking up on a point from Dingledine's presentation. In outlining Free Haven's design for anonymous file storage, Dingledine had mentioned a key problem with realizing their vision—whenever you have a censorship-resistant publishing system, you need a way to communicate anonymously. As Syverson told Dingledine, this was something he and the NRL had been working on for some time, and he invited Dingledine to work on onion routing, to try to take the first steps towards making the Free Haven dream a reality. If they could get a shippable version of onion routing ready, and fast, they could attract more NRL funding for the work that Dingledine wanted to do—programming privacy technologies.

At this point, Dingledine and Mathewson were working for a start-up, Reputation Technologies, with Dingledine holding the job title of "security philosopher." Reputation Technologies, formed by Rich Lethin and Roy Rosas, was by this point mostly focused on business supply chain analytics, but had attracted first Mathewson and then Dingledine (and its initial funding) with the rather lofty goal of eliminating dishonesty as a viable business practice by creating a complex technical infrastructure for managing reputation and trust in anonymous contexts. With a loyalty that seems, in retrospect, quaint compared to the cutthroat tech start-ups that would come in the years to follow, Dingledine leapt at the chance to join the NRL's efforts but made clear that he wouldn't abandon his friends at Reputation Technologies. So rather than poach Dingledine for the NRL, they hired Reputation Technologies as contractors to work on the next generation of onion routing.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Beginning work on a publicly releasable version of Tor, Syverson and Dingledine set to work, pulling together a loose set of people from the crypto community around a mailing list—*or-dev*—where, while the core team hacked directly on the code, the rest could contribute to design discussions, carry out tests and experiments, and generally provide advice on what might actually work in practice. In mid-2002, discussions on the list began between a small group of developers. Among the most involved early contributors were a host of people who would go on to make their names in industry and academia: Andrei Serjantov, Bruce Montrose, George Danezis, Matej Pfajfar, then later, Rachel Greenstadt and Marc Rennhard. Some of the original cypherpunks, in particular Lucky Green, would also take part.

As with many of Tor's technologies, the first stages of the Tor protocols were rooted in almost comically modest beginnings. Matej Pfajfar, then a Cambridge computer science student, and now, at the time of writing, a senior engineer at Google, had put together a working model version of a "second generation" onion routing network as an undergraduate dissertation project. This, based on the test systems created by the team at the NRL, formed the starting point for Tor, with Pfajfar conceiving of a neat workaround with the NRL to allow them to publish all the code in real time with an open license.[11] But creating a real onion routing system required more than an abstract design and a toy network. Like moving from an architectural diagram to a real building, decisions needed to be made about implementation, and then the digital bricks and mortar need to be laid in the form of working code.

> We've got OR code that works and seems robust to basic use. Now's the time to figure out what features we actually want, and how hard they'll be to get.
> Roger Dingledine—or-dev, Jun 2002

Although the core design of onion routing was well advanced, a number of important decisions about its implementation in a real network remained up for discussion when the small group of developers got together in 2002. These decisions about the design of Tor would have important consequences, including about the protections it would give, who would be able to use it, and, most importantly, the enemies it would protect its users against.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Answering these questions would also provide a focus for the collision of Tor's early community and cultures. The first year of Tor's development, they decided, would focus on refining Tor's *threat model*—a set of design principles that would package up the intended users and use cases that Tor would try to support, and the attacks and attackers against which it would try to defend.

The developers weren't starting from scratch, but instead had learned from years of concerted hacking on the onion routing design by a range of groups. Teams working on Tor's competitor anonymity projects had been working through many of the same design problems that the Tor team would face, but often came to different conclusions. This meant that designing Tor was more a process of configuration, of evaluating a series of design trade-offs, than developing something brand new. These issues ranged from technical design features to more prosaic concerns, such as how to fund such a service. For-profit, pay-to-use services like Zero-Knowledge Systems had little appeal to the public—however much people valued anonymity, few were willing to pay for it. Similarly, a whole host of potential designs existed for a relay network—some projects allowed anyone to join the network, while others required sign-up with official identification.

The problem was that no one had yet found a way to build a system with appeal beyond a tiny crowd of technical nerds. The systems competing with Tor were mostly designed by cypherpunks, and for cypherpunks, security would always come first. They assumed that the best way to increase their user base was to maximize the protection it provided, and couldn't imagine a user who would accept a less secure system. But in an anonymity system, the more protection you add, the harder (and paradoxically, often less secure) an anonymity system becomes to use. The technical defenses you need to protect against strong attacks in an anonymity system tend to slow it down and make it far less stable, creating bottlenecks where it can get overloaded.

In Dingledine's own master's thesis, however, there was the seed of an answer. As he identified, there were a range of genuinely popular, mass-use decentralized systems at the time: Napster had 80 million users in 2001, and LimeWire and BitTorrent were similarly successful (even though they provided no anonymity at all). So there *must* be a mass user base for an anonymity system, if only they could figure out how to build—and sell—it right.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

So, far from being authored solely out of the fevered dreams of the US military, as some have claimed, Tor was only the most successful of a range of projects, all furiously trying to solve the same few design problems and develop an internet anonymity system that the public would actually *use*.

In fact, it was this panoply of competitors that gave Tor its name. To distinguish their work from the various other anonymity networks using onion outing, they decided early on, with the blessing of the original team, to make clear that they were the "real deal." On the mailing list, in 2002, they named themselves Tor—in other words, *The* Onion Routing. Even years later, getting this wrong (by calling it The Onion Router, or writing TOR rather than Tor) remains a surefire way to get tripped up by the security community.

In these early days, the Tor developers spoke a lot about who might use their system. Core to any threat model (and more broadly, the design of any technology) is a model of the user. The mailing lists abound with different examples: someone accessing the *New York Times* website from China, a protester on the streets of the US, or a spy (endearingly termed a "road warrior") deep in hostile territory. But in terms of a *model* user encoded into the design of the system, the Tor developers tried to remain as agnostic as possible, leaving it open to an enormous potential set of global users who could use it for all aspects of their online lives, even future ones (such as online pizza delivery) that didn't exist at the time. This built-in diversity was a critical feature of the protection offered by Tor—the users and uses would be so diverse that an attacker couldn't tell anything about the user simply by seeing that they were using Tor.

However, as generations of engineers have learned the hard way, designing a technology for everyone is much like designing it for no one. The onion routing paradigm itself begins with a strong, if very basic, model of potential users split into two rough types implicit in its design. The first of these we might call "everyday privacy" users—privacy-conscious people who use Tor every day for a wide range of different reasons, most of which aren't illegal or suspicious at all. These everyday users are surveilled by governments and corporations, but not in a particularly targeted way. Instead, powerful actors are looking at those users as a tiny part of a huge sea of internet traffic that they are trawling for activities that could be either illegal or potentially

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

exploitable for cash. These users form the enormous bulk of Tor traffic—the "cloud" of cover traffic in which our second user type can hide.

This second type of user includes the people who could appear in blockbuster action films: "high security" users, or people for whom Tor is a lifeline that could protect against arrest or even death. We might think here of whistleblowers like Edward Snowden or Chelsea Manning, revolutionary activists in repressive regimes, or spies attempting to "phone home" from hostile territory. For these users, government surveillance is targeted, immediate, and potentially deadly. The traces left by their communications and browsing habits are scrutinized in depth by powerful actors looking for clues as to what they're doing. And the consequences can be deadly, from dawn raids after an inadvisable connection to a particular web forum to drone strikes based on patterns of telephone and internet traffic. When former head of the US National Security Agency Michael Hayden said, "We kill people based on metadata," this is the group of users that he meant. It is this kind of extreme threat from which Tor tries to protect this second group.[12]

But another kind of "user" was still lurking in the background of these discussions. The view that security engineers have of a technology has a crucial difference from other forms of design. While regular users are still important, much of a security engineer's time is occupied by thinking about adversaries, a special kind of user who wants to either break the system entirely or subvert it to achieve dangerous or undesired results well outside of the design specification.[13]

Who were Tor's adversaries in 2002, when it only existed in the minds and hard drives of Roger Dingledine and his collaborators? Surprisingly, sifting through the design documents and emails, it becomes clear that Tor was never designed against particular enemies. Reflecting the divisions of geopolitical power at the time, the design discussions rarely mention, for example, what capabilities they think the Russian or Chinese (or, for that matter, American) secret services had or might gain. Although the NRL were still involved, intelligence about real adversary capabilities—what the Chinese security service were able to do, or what the Russian intelligence services were exploiting in the wild—is almost never mentioned. Instead, Tor was designed against *structures*—attacker models rendered in the abstract.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The first set of discussions preserved in the mailing lists set out these models of different attackers in great detail. One of these turned out to identify a fundamental weakness with the onion routing design. Despite the internationalist visions of a relay network of volunteers around the world, Tor's power relies on an internet where control is fragmented among nation-states, each of whom controls only a fraction of the whole and is not predisposed to share intelligence with another. This means that even if one of the Tor relays you're using is in the United States and being monitored by the National Security Agency, the other two, which might be in Russia or Estonia for example, won't be. Even if the Russian and Estonian governments are watching their own internet, no single actor has access to all three—which is what you need to reconstruct the path through an attack type called *traffic analysis*.

But if an adversary has a global view of the internet, able to spy on your nodes no matter what country they're in, you have a real problem. Called the *global adversary*, this adversary, with an extensive purchase on the internet infrastructure around the world, is Tor's great weakness. And while this was a mere theory in 2002, over the next ten years, the United States would become just such an adversary.[14]

Fortunately for Tor's designers, the global adversary comes in a range of flavors, some harder to beat than others. In these early days of mailing list discussions, Syverson and the other developers sketched out three broad kinds of global or near-global adversary. The first of these is the most powerful: the *global active adversary*, who is able to see all traffic on the internet, from the Tor nodes to the users' computers, and can also modulate the signals those users send. This means that they can add little identifying delays and signatures to particular people's traffic in order to deanonymize them, as they can spot the tagged traffic coming out at the other end of the Tor network. This is almost impossible to beat; although some designs (like mixnets) try to tackle this by holding signals at the nodes and releasing them at random in batches, the defenses add so much delay to the system that they would render normal web browsing impractical.

The second type of global adversary is less powerful, able to see everything on the internet but not able to change it. These passive global adversaries can perform what are called *timing attacks*, collecting huge amounts of

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

traffic coming through the onion routing networks and then using complex statistical correlations to trace the routes back to their destination. The existence of something like a real-life global passive adversary was later confirmed by the Snowden leaks, which revealed that the US government had been using its strategic hold over the backbone infrastructure of the internet and the US-based companies that had spread their services around the world in order to spy on a huge percentage of global internet traffic. Most anonymity systems around at the time tried to beat (or at least frustrate) this global passive adversary through a range of approaches, often involving sending fake packets of data through the network to confuse their calculations.

The third kind of adversary was the most realistic (at least in 2002) and the easiest to beat: the *roving adversary*. This adversary has a core network that they surveil, and which may be large but is generally limited by global conflict, fragmented ownership of digital infrastructure, and limited sharing of intelligence. With these limitations, the adversary is able to compromise other parts of the internet by hacking computers, but needs a budget in order to do so and is often unable to hold onto them for very long, as operators patch their systems and kick them out. Tor is a real problem for this kind of adversary—as long as the network has some relays in hard-to-reach places—but a range of options still exist to add more protection.

The onion routing design, as well as other anonymity systems, includes a standard way to beat these global adversaries and their timing attacks through the use of so-called *padding traffic* (rather than the randomized delay used by mixnets). There are lots of different ways to do padding, but they all involve sending fake data around the Tor network in order to confuse attackers. Some of these are extreme, like potential designs in which every Tor relay constantly sends as many padding cells full of fake data as it can to all the other relays, and users must remain online and broadcast this padding constantly to hide when they join the network for real. Other approaches are more simple. For example, relays can occasionally make fake connections to one another or mix in a small amount of padding.

As the developers began to play around with different designs for their real-world onion routing system, they initially assumed (because all the other projects so far had) that some kind of padding would be an absolute

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

necessity. The power of the global adversary—synonymous in the minds of the cypherpunks with the omnipotent digital authoritarian nation-state of their nightmares—was too sinister to be dismissed. So the Tor developers would spend the first several months of development trying to evaluate whether there was any system they could design to beat it, while keeping Tor as a whole usable enough to appeal to the general public.

Figuring out what sort of padding system might work was extremely complicated in practice. Even from just the emails sent between this small community of computer scientists twenty years ago, it's clear that the existing ways of thinking about crypto systems didn't work very well for onion routing. Usability and anonymity exist in tension in onion routing. Usability improvements generally increase anonymity in some senses, because they lead to more adoption, but they can reduce it in other ways if they make the system less secure to some kinds of attacks or if they make it easier to poison the system or shut it down.

A crucial aspect of engineer culture is measurement—pinning the butterfly of the social world to the board of a technical system. How do you take a rich and abstract thing like privacy and measure it in the language of computer technology? From the start, it meant balancing a number of different factors, trying to measure and evaluate the "overall" amount of privacy that a particular design would provide. The models available from cryptography weren't necessarily suited to the task.

Many of the developers had trained as cryptographers, and this culture exerted influence. They felt like they needed to measure Tor against the same kind of models as they would for a cryptosystem. They began by drawing from the approaches that cryptographers use to talk about these systems: measuring anonymity in raw numbers and rendering privacy as abstract mathematics. When working with information systems, it makes a certain amount of sense to think of *everything* as information. This allows you to take information theory and math and use them to describe the "real-world" properties of your system.

Privacy as a problem of information and information flows exists to a cryptographer through the idea of the *anonymity set*. If you have a system with one thousand users, all of whom are indistinguishable from one another

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

to an observer, your chance of correctly identifying one of them is one in 1,000—this is your anonymity set. So a system with 2,000 users would have more anonymity—the increased size of the crowd means that you have a one in 2,000 chance of correctly identifying your target, rather than one in 1,000.

Applied to a practical system design, we can get fancier. If your Tor user base has 1,000 users, but an adversary can identify your operating system, then you have a problem if only three people use a Windows computer. This adds *structure* to your system, making it easier to reason about. Your adversary can effectively use this structure to split these users off into their own group—their chance of identifying a Windows user is now one in three. When you bring in more dimensions, such as time, things get even trickier. If you know that your target comes online between three and four o'clock most days, you can begin to build up a signature of their traffic patterns and identify them in the network mathematically.[15]

The idea of the anonymity set gave Tor's developers a basic way to reason about the effects that different kinds of padding might have. They could make mathematical comparisons in the abstract and then take measurements of test systems and simulations based on how their designs and practical operation affected the size and structures of user anonymity sets. But these "pure" models began to break down as the Tor developers worked through the scenarios that could come into play in real life.

> The types of argument you see in cryptography is like, imagine [the adversary] could build a computer with all the atoms in the universe, what could they do? And so you come up with an extremely strong threat model, and then you build your system, and you show that within this threat model, it's secure . . . the problem with anonymity is that we can build such threat models, stronger than any adversary, but then we don't know how to build a system that actually works, or is usable in that case. So the threat models in cryptography are quite different to the threat models in anonymity, not just in what they are, but in how they're developed.
>
> Tor core developer

Any state can break Tor fairly easily by installing a spy camera in a person's bedroom, compromising their phone with malware, or engaging

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

in "black bag" or "rubber hose" cryptanalysis (physically stealing someone's computer or torturing them until they reveal their passwords). But Tor aims to prevent mass-scale analysis of people's internet data. And nation-states—in Syverson's words, "the Man"—have budgets, agendas, and resources.[16] In the context of the early 2000s' War on Terror, this budget was effectively unlimited for some targets considered particularly threatening. The methods they use in practice aren't abstract math problems carried out on a sea of indistinguishable users, but analysis of complex, patterned behaviors based on available resources and the bits of the internet they're actually able to control in practice. The internet isn't a "flat" hyperspace of power, but a rugged landscape with an extremely fine and complex structure.

Tor complicates and transforms this landscape of power but doesn't flatten it to nothing. The nodes themselves still sit on the internet and follow its topologies. Figuring out the real anonymity and security Tor might provide requires working out, case-by-case, a range of different scenarios in fine detail, understanding exactly what the internet infrastructure looked like at each stage of the journey into, through, and out of the Tor network; how it was being used; and how it might be compromised. In other words, it requires understanding the real knots of power and infrastructural control that the adversary might be able to deploy, as well as the real shapes and patterns that the users would create in the network that might be used to identify them. Some nodes might be trying to spy on you, some destination websites might add malware to your computer to track you, some parts of the network might be faster or slower than others, some users might look very distinctive—all possibilities that made an entropy calculation very hard in practice. A real-world adversary might simply shut your network down by overloading it with traffic or poisoning it with slower nodes. In other words, approaches from cryptography didn't work well as a measure of *privacy* for the very people the system was trying hardest to protect.

> [entropy] is not a realistic view of how large, widely used anonymity networks work. They are comprised of fairly dynamic and diverse collections of users communicating over nodes that are diversely trusted by diverse parties and that are diversely configured versions of diverse platforms. And these nodes are

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> connected over diversely trusted links (based on ASes, ISPs, geography, etc.). Unlike designing a closed secure system, there is no point in even discussing trying to make the degree of security of all of the different parts of the network roughly comparable.
>
> Syverson, P., Why I'm not an entropist[17]

As these more complex scenarios were brought in, especially where ideas about trust, motivation, and behavior were represented, the developers needed to be able to weigh these social, technical, and mathematical factors against one another. They did this by developing, bit-by-bit, a way of transforming the properties of users and adversaries into technical representations by mapping them as topological patterns of information, power, and risk in the system.[18]

> Informally I think [the roving adversary] reflects the capability of an attacker to root several machines very quickly but can't hold on to them for very long (sysadmin having a late night and figures out something is going on or some other form of [intrusion detection system] etc).
>
> *or-dev mailing list 2002*

> But, what is reasonable in [the roving adversary] is the partial compromise of the network. An adversary has a budget, and short of a systemic vulnerability, he must compromise individual network elements or set up his own.
>
> *or-dev mailing list 2002*

Developing this more bespoke approach to mapping their system allowed the developers to assess the practical consequences of different implementations of padding traffic for usability, resilience, security, and a range of other factors. The developers used these design practices to reason about how long it would take to deanonymize different use cases, mapping out the information structures and patterns in each case:

- If there are more users, it may take longer [to deanonymize them].
- If Alice's behavior isn't very odd (that is, if she behaves similarly to other users), it may take longer.
- If other users are online more often, or Alice is online more often, or Bob is online more often, it may take longer.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

- If Alice sends requests to a bunch of people besides Bob, it may take longer (or it may not improve anything at all—wouldn't it be neat to be able to show that.)

If Alice refrains from talking to Bob as often, then it may take longer.

or-dev mailing list 2002

Once these representations were formalized, the developers could engage in "attack brainstorming" by stress testing each use case and trying to work out the consequences of different kinds of attack or adversary—what they might be able to achieve, and which attacks they might be able to prevent.

> It's like, someone presents a solution to this problem. And then usually what happens is that a bunch of people think through this and then come up with attacks to it. Um, and it's like, hey, what if someone did this, what if someone did this, what if someone did this? And you kind of iterate on it until you come to a point where all of the attacks you can think of in this space fail against your solution. I mean, unless someone comes up with something that's completely different, or comes up with an attack that completely subverts that, that is your working model of how things are going to be.
>
> Tor community developer

So they could see the effects, for example, of having every computer connecting via Tor send random packets of fake data all the time, or having the nodes on the relay network fill their connections to the brim with padding traffic to hide the real signals. They interrogated each of their core adversary and user categories in this way for a range of different padding designs, mapping different potential geographies of information and control, and the consequences for Tor's users in each case.

As they worked through these different scenarios, refining their abstract user and adversary categories, a conclusion began to emerge—a *material* constraint on the effectiveness of their system. Firstly, the everyday types of online activity that they were trying to protect were inherently patterned: users want to speak to the same people repeatedly, have long-term and linkable relationships, and regularly visit the same websites. The traces left by these activities are extremely distinctive, providing attackers with a wealth of different ways to characterize individuals and deanonymize their Tor traffic. As they mapped

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

these patterns in practice, they concluded that protecting against all traffic analysis attacks would require a degree of padding so onerous that the network would be unable to support everyday browsing, incredibly slow, and easy to render unusable as it would already be clogged up with padding traffic:

> Here's my point about padding. Right now I'm not convinced there can be padding/throttling regimen that is both useful and practical, or maybe even either useful or practical.
>
> or-dev mailing list, 2002

Secondly, as they refined their adversary categories, they realized that the idea of the global passive adversary was both "too weak and too strong." In practice, a global view of the internet is extremely difficult for even nation-states to attain. Even discounting the difficulties of getting taps on all the internet "wires" around the world (for example—you can tap the sea cables between continents, but this doesn't give you traffic traveling within countries), the enormous complexity of autonomous systems and internet service providers and the rest of the "internet geography" mean that without the helpful identifiers of IP addresses, tracking signals around the internet is very difficult. Equally, they realized that any adversary that is genuinely able to maintain a global view of the internet passively would have access to a range of other "active" attacks—such as delaying or modulating signals entering and leaving Tor nodes—that padding does nothing to stop.

> I have a basic problem with the idea of global passive adversaries. As an academic exercise, it seems fine, but it is hard for me to imagine an adversary that is powerful enough to be global but weak enough to be entirely passive . . . The global passive adversary is a fairly clean notion so perhaps it should still be pursued for abstract analysis purposes, but I need way more convincing than I've seen to design against it.
>
> or-dev mailing list, 2002

> In the end, what we said was . . . because it's so easy to do the end-to-end timing correlations, we weren't going to bother to add overhead of any . . . padding, until somebody could come up with a design where we thought that it was reasonably helping to, to raise the bar. You know, so that it was actually worth it.
>
> Tor core developer

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

This led the developers to remove padding traffic and global adversaries from the design of Tor entirely. Instead, they concluded that, rather than a global flat terrain filled with indistinguishable users, a realistic adversary would be faced with shifting, localized, partial views of the internet. Tor could make this picture a lot more complicated by taking unpredictable routes through a random selection of countries that might or might not be observable, and by getting as many users and relay operators involved as possible.

This gave them a justification for turning off many of the highest security features of the system design. The cypherpunk contingent, however, was initially less than enthusiastic about this compromise. Lucky Green, a long-standing presence on the Onion Routing Project, argued (in the colorful style of many of the cypherpunks) that a system with anything less than the strongest practical protections would fail to convince enough expert early adopters to reach critical mass at all. This approach lacked the formal proofs and direct numerical outputs of more traditional cryptographic scholarship—and so would be a hard sell.

> [. . .] my personal feeling is that any kind of scheme needs an analysis of anonymity in some kind of formal way and statements like "probably resistant against blah" just don't cut it any more. Research that unfortunately so far appears to remain missing in the area of IP anonymizers are quantitative analyses of the impact the various approaches have on the aspects that together make up our notions of "anonymity" and "privacy" . . . This is what I believe killed Z[ero-] K[nowledge] S[ystem]'s Freedom. The early adopters knew that the system was insufficiently secure against a resourceful attacker. ZKS, erroneously, believed that in producing a product that defends against some percentage of attacks, say 98%, they could capture most of the of the market. Instead, Freedom captured about the same percentage of the market as human blood transfusions guaranteed to be 98% free of HIV virus would. Some product groups offering 98% security do not just capture a slightly reduced market share, but experience difficulties to find any market at all. Anonymizing systems fall into this category.
>
> Lucky Green, *Or-dev* mailing list

But this was to no avail—padding was soon gone from the Tor design. The consequences of not including padding were immediate. Tor looked much like many of the other systems around at the time, but with most of the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

most onerous security design "switches" (padding, mixing, delays, registering operators) turned off, massively improving its usability and speed. This is one reason that Tor survived—many of its competitors, developed as they were by cypherpunks for whom security was the ultimate goal, prioritized resistance to powerful adversaries over usability. The high-latency projects all more or less could not handle web browsing, but instead only email and other use cases where speed was a secondary concern.

Unlike encryption tools, the anonymity from anonymity networks is proportional to user numbers, so they have a tendency to "death spiral"—they cannot sustain a low number of committed users, needing a minimum carrying capacity to function usefully. Tor, shaped as it was by both a cypherpunk desire to protect against state intrusion and a military-academic pragmatism, was able to mobilize the powerful network effects of an increased user base to achieve a large enough size to genuinely grant its users practical anonymity.

Out of this soup of ideas and practices, fusing the techno-radicalism of the cypherpunks and the military-academic practices of the NRL researchers, Tor's distinctive privacy world was emerging. This set Tor apart from its competitor projects. Where the others often prioritized a pure cypherpunk technical maximalism, the Tor developers brought this together with a healthy dose of the pragmatism that characterized the military-academic world. While the cypherpunks often displayed this pragmatism when breaking down systems built by other people, structural ideals often became the end rather than the means when they set out to build their own systems. But Tor's developers quickly came to realize that trying to make the system as secure as possible in theory would make for far less privacy in practice.

As Tor's developers tried to wrestle with mapping out different designs and their consequences, they increasingly put together a rather novel way of thinking about what technologies like Tor should be and how they should act on the world. The vision of privacy you get through the entropic eyes of the military cryptographer, of a hunt for a target within a sea of anonymous souls, is rather different from that imagined by Tor's design. We can think of this as its own privacy world—which I call the world of the *engineers*. At its heart is an idea that works like a key or cipher—a single concept through

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

which the whole universe can be translated into the language of Tor's tech. This idea can be summarized as *privacy as a structure*.

> I see the work that I do as decentralising and distributing power. Because I think that's always a good thing [*laughs*]. I see that as a fundamental . . . like, if nothing else is true in the world, distributing power in this world is a good thing. And, so . . . when you're threat modelling, it's a case of, how do we take this cluster of power here . . . and how do we remove that from the equation?
>
> Onion Service developer

As the developers mapped out the enormous complexity of the internet landscape, they found knots and microstructures of power in the roots of the internet's physical forms, below the abstract topologies of "decentralized" systems. Design then became a game of finding practical ways to work around those microstructures. This way of building a system was bound to its own understanding of privacy: as a dense topology of material and structural power in the complex networks of modern information systems that their users' signals would have to navigate. In this vision, states and corporations exert power through their material control of the network,[19] and privacy can only be reclaimed through re-engineering the microstructures within this network of power. This is an extremely powerful way of thinking about privacy, and one that extends not only to networks and technologies in which power can concentrate, but to networks of people as well—their own network structures, patterns, and clusters of power between one another and within the traces they leave in the internet. We can even see the echoes of this perspective in the ways that the engineers talk about wider issues of internet freedom:

> I think privacy does level the board a bit. So, I think privacy helps weaker people, it helps people who want to enact change. Powerful people do not need privacy to the same extent, because they have other means of defending themselves against bad things happening. So, I think it is also a technology that tries to help equality.
>
> Tor developer

The nascent Tor engineers articulated a vision of privacy beyond the pure strategic pragmatism of the military-academic world and beyond simply

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

US global power, retaining the utopianism of the internet freedom movement and a powerful vision of the future internet. This also had far wider ramifications, providing a language which, as the project evolved, would be used to talk through the other conflicts Tor would face in its early years. This language was powerful but flexible enough to engage a range of different political groups that were clashing over the internet as the 2000s wore on. The idea of privacy as a network structure meshed as easily with the hacker community's libertarian views as it did with the liberal (and neoliberal) designs of US foreign policy, and even the more radical liberation struggles that began to bubble up as a new generation of political movements discovered the internet.

This engineer privacy world would come to define the early years of Tor, and to this day encompasses what has throughout its life been the core contradiction within its community: finding a way to make the global ambitions of US geopolitical power fit with the radical (and often explicitly *anti-colonial*) politics of techno-libertarians and high-tech anarchists. Incredibly, the engineer world of Tor's developers managed to unite these in more or less a single culture—one which persists to this day, in which grungy crypto hackers and hyper-cool anarchists rub shoulders and speak a common language with people with US military email addresses.

With this conceptual framework now established and the biggest design hurdle cleared, further design decisions followed quickly soon after. Tor's foundational culture—the *engineer* world, a hybrid of the military-academic and the cypherpunk cultures—began to stabilize and lay down roots, as an approach to anonymity engineering that underpinned a whole way of seeing privacy and digital technologies. Guided by this emerging culture, the developers experimented with a range of different features—for example, contemplating allowing users to easily choose how many "hops" their traffic should take through the network. This too would fall by the wayside—although it might have allowed some people to customize their own level of security, it would make the software more complicated to use and potentially make their Tor traffic look different from everyone else's, segmenting the network. Instead, the developers settled on a three-hop design, with everyone's traffic passing through an entry, middle, and exit node—the minimum

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

distance required for onion routing to work. Wherever more complexity, or the opportunity to confuse users with a less or more secure mode popped up, it was generally considered and abandoned. As Dingledine said:

> That's a really good point. It was rolling around in the back of my mind, but I hadn't followed it to its conclusion: "If I implement a 'stupid mode', most people will turn it on."
>
> Roger Dingledine, or-dev mailing list, 2002

As this design work was taking shape, Dingledine and Mathewson were laying out the software foundations of what would become Tor's first set of public releases. Underneath this high-level design work, much of what was needed was the same kind of software engineering that would underpin any project with a broad user base: handling data, building foundations and core modules, producing documentation, testing, and fixing bugs. Mathewson was living in a converted apartment in an attic in Cambridge, Massachusetts while Dingledine was across town, closer to Harvard Square, living with Rachel Greenstadt (herself an extremely prominent privacy academic, engineer, and contributor to the Tor design work). Debating the various aspects of Tor's design on instant messaging chatrooms, over phone calls, and on walks through Boston, Dingledine and Mathewson would also spend hours at one another's apartments, working from coffee shops and through long evening sessions as the contours of Tor's first release took shape under their fingers.

A first open version of Tor was ushered into the public eye on Dingledine's Free Haven website in 2003. Over the next few years, there was an explosion of academic and technical work around Tor. Some of the biggest figures in crypto hacked on, reviewed, developed, and tried to break the early Tor design.[20] Dingledine presented an initial paper on the design at the USENIX Security Symposium in 2004, and subsequent papers at Information Hiding Workshops, the Workshop on the Economics of Information Security, and the Privacy Enhancing Technologies Symposium would come to solidify the emerging technical design of Tor as a set of formal proposals and new kinds of knowledge about secure systems for others within the field to take up or attack.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Although Tor would break away from the pack in terms of popularity, it retained its links to the other anonymity projects at the time—getting feedback from them, integrating clever designs solutions they were developing to shared problems, and building inter-operable interfaces and standardized components so that their systems and networks could talk to one another. But Tor development remained difficult work that was hard to express in the frameworks that cryptographers had developed up until this point. For a long time, even the core security model of Tor wasn't developed into a formal proof of the kind that was typical for other cryptosystems—this took until 2007.[21]

The utopianism of the early web pioneers, the cypherpunks, and (in a rather more practical form) the US military-academics can be readily seen in these early days of Tor, both in the culture forming around the engineers, and in Tor's design itself. Across Tor's history, many people would come and go, but Syverson, Dingledine, and Mathewson would drive much of its direction, acting as a mix of lead developers, institutional conscience, and, occasionally, benevolent dictators. As Dingledine's hunches about file-sharing were proven right and a public market for their anonymity system started to grow, the new power structures they were building began to spread around the world. But a new group of people was slowly joining the network—and they had ideas of their own.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

5 ENTER THE MAINTAINERS

As Tor was eased out into the world, it needed more than just a design and a repository full of code. Unlike a standalone computer program that could simply be written and then distributed to its users with occasional ongoing updates, Tor needed infrastructure—a real network of servers around the world around which it could bounce its users' signals. As the infrastructure studies scholar Susan Leigh Star tells us, where we see an infrastructure, we often *don't* see the huge amounts of vital hidden work and maintenance lying under the surface.[1] Underneath the Tor design and code, first dozens, and eventually thousands, of people around the world were (and still are) working to keep the network alive. Without these hidden people and their work, Tor wouldn't exist at all.

The relay network is a very odd form of infrastructure—a highly dispersed and fragmented network of parts with little central control, but which nonetheless has managed to achieve stability. What the Tor network relies on above all else is a bizarre, chaotic community of relay operators, volunteers who maintain the nodes and provide their bandwidth to the network. From these practices, and from the ideas and values percolating through hacker and maker communities across the first decade of the twenty-first century, emerged a rather different understanding of what privacy might mean in the context of Tor. This was a second privacy world, loosely bound to the world of the engineers but with little time for their pretensions to techno-revolution and a radical restructuring of society. Instead of *privacy as a structure*, it saw *privacy as a service*.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Joining the Tor network—becoming a Tor relay operator—is easier than one might think based on common perceptions of Tor as a shadowy crime technology.[2] Nearly anyone can set up a Tor relay using software downloaded from the Tor Project website—in its simplest terms, you download a program, configure some options, start running it, and you're part of the Tor network. You can run it on your own home computer (though this is generally a very bad idea if you're running an exit relay, for reasons discussed in Chapter 8), but most people buy a private server and set it up there, where it won't go down if their home internet connection gets patchy or someone spills Coke on the router. Once it's up and running, the relay sends a signal to something called a *directory authority*—a service run by one of a few people trusted by the Tor Project who keeps a list of all the relays currently in the Tor network (this is also called the *consensus*).[3] From this point on, when someone boots up their Tor browser, the new Tor node will be on the list of relays that their browser downloads and could be used in a Tor connection.

Some of this participation is admittedly mostly symbolic. The algorithms that govern the Tor network mean that newcomers are treated with suspicion—and with good reason. A malicious operator joining the network could set up large numbers of relays and then begin collecting the IP addresses of people connecting, over time gathering enough data to begin to deanonymize them. Equally, a new relay might simply not be very good, dropping connections a lot, spending a lot of time offline, or providing a very slow service. This might happen by accident—simply a newbie running a poor internet connection. But it could also happen on purpose—a security service adding lots of dodgy, malfunctioning relays to poison the network. Thus, the distribution of traffic on the Tor network is shepherded by balancing algorithms working behind the scenes. Most new relays take some time to convince these algorithms to allow them to handle more than small amounts of traffic, with most circuits passing through a few hundred extremely stable, high-bandwidth nodes. In addition, a team of bad relay hunters at the Tor Project regularly inspects the network, kicking out any relays that they think look suspicious.

In gathering the first pieces of the relay network, Tor was reliant largely on word of mouth to get enough people enthused about the project to

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

contribute. They pulled together contributors from the existing remailer and anonymous routing projects at the time, including some from Dingledine and Mathewson's old Mixminion community and a larger group of dedicated cypherpunks and anonymity experts who wanted to help. Dingledine was adamant that the relay network be kept totally separate from the team developing Tor itself—that the relay network not control the infrastructure as well as the code because this would require the users to put too much trust in a single group of people. Despite this, for the first few years, the team knew most of the relay operators by name.

At the USENIX symposium in 2004, the team formally introduced Tor to the security research community. They described the early network, as it existed in 2004—a mere 32 relays, mostly in the United States and Europe.[4] They estimated based on their traffic statistics that they had a few hundred regular users of the network, including at least one who had set up an early hidden service (the original name for onion services, later changed to make it sound less seedy), hosting a wiki page.

Expansion over the next few years was piecemeal, with relays added in fits and starts after a talk by Dingledine at a tech conference or a particularly high-profile news article inspired groups and individuals to start contributing to the network. Things really took off in 2005, as Tor's institutional structures, connections to the hacker scene, and users in the digital rights community flowered (as I discuss in the next chapter). University system administrators and computer science departments, sometimes already using the Tor network for research purposes, began to set up nodes themselves, along with libraries, digital rights NGOs, software foundations, and a range of other groups with interests in digital freedom, anti-censorship, and anonymity, and who often had substantially more computing power at their hands than an individual operator might have. By 2009, the network would count more than 1,500 relays.

The so-called "hacker underground" was an important source of new relay operators for the growing Tor network. By the 2000s, it had evolved from its scrappy 1980s roots into a loose but large agglomeration of different communities and cultures, many rather different from what had come before.[5] Most of the people involved in for-profit cybercrime schemes and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

online fraud were leaving the hacker scene; they were generally not that interested in the technology for long once they started making money, but the people who stayed around shared a profound love of technological experimentation.

The contemporary culture of this underground hacker scene has been well documented by anthropologists and social scientists, not least because it involves some of the most enjoyable fieldwork sites available to digital researchers. Although this group spent their time in a range of online spaces, crammed into crusty local hacker labs and bedrooms around the world, there is a long-standing tradition of freewheeling annual conferences and camps.[6] From the Chaos Communications Congress in Germany (running since 1984), to the Electro Magnetic Field camp (held in a damp English field since 2012), to Hackers On Planet Earth in New York (since 1994) and Defcon in Las Vegas (since 1993), these joyous, controversial, and messy events are a site of annual celebration for a loose community of people united by an interest in breaking and repurposing technology of all kinds. They feature robots and late-night raves, lockpicking and leaks, and, more often than not, a dedicated Tor stall, talks from the Tor Project, and a meet-up for relay operators in the community. These conferences became places where the growing Tor community could meet up and socialize, encourage others to set up a relay, or petition the diverse array of software projects and hacklabs (who often set up their own stalls, complete with custom stickers and T-shirts) to join the network as well. It was also a place where the Project could make connections with the wider hacker community and find out how people were actually using their software.

As more people joined the Tor network, it began to take shape as a loose and heterogeneous global community. The Tor network today links together aluminum server racks in French data centers; tiny Raspberry Pi computers sitting next to bottles of German lager in a sixteen year old's bedroom; octogenarian IT security professionals' home systems covered in blinking lights and stickers; unassuming computer towers that provide a footrest for activists when they get back home from an underground rave; and clandestine servers sitting underneath Pink Floyd posters in university computer labs, registered in a budget line as "miscellaneous computing resources."

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Its wires stretch through dozens of countries and across a mess of different operating systems and configurations. And although now the core of the network carrying most of the traffic is pretty slick and professionalized—a few hundred very high-capacity servers in big data centers—this scrappy alliance of bedroom projects and smaller servers still exists at the edges of the network, and still plays a vital role in keeping it alive.

I spent most of the first year of research for this book, in 2016, interviewing relay operators, myself still fairly new to and not known at all by the Tor community. Hanging out on instant messaging channels, posting on mailing lists, and generally annoying people, I initially encountered a lot of resistance, with people often assuming that I'm a covert FBI agent or undercover spy. But as the months wore on, more and more people agreed to speak to me. It struck me as quite an odd group—I met techno-libertarian tinkerers, unabashed fascists, card-carrying liberal democrats, and anarcho-socialists. What they shared was a general interest in technology and digital privacy—most of the relay operators I interviewed had at least some background in IT, whether as a hobbyist programmer, a systems administrator, or a security consultant.

Outside this core of enthusiastic geeks were a scattering of other, more varied perspectives: human rights lawyers, digital freedom activists, and others who supported the political goals of the Tor project and had the basic technical skills to follow a how-to guide on setting up a relay. However, given the commitment required to run a relay, many in this less technical group tended to move over time instead to donating money rather than time and bandwidth to Tor—either to the core Tor Project itself, or to one of the relay operator co-operative organizations that had been springing up.

But despite the technical background of many operators, their understanding of the workings of Tor itself—the code, cryptography, design, and development—was minimal. When asked how well they understood how Tor worked, the operators I spoke to took care to make the distinction between their knowledge of network administration (the functioning of the infrastructure, their own machines, and connections between nodes) and the inner workings of the Tor code, which was of less interest to them. Even the operators with more technical knowledge saw this as the job of the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

core project developers and academic researchers—not something the relay network should worry about.

> I do not follow the development. I think they know what they are doing and I am not a coder.
>
> Tor relay operator

This somewhat puts the lie to Tor's "open source" vision—transparent might be a better term. Unlike Linux or other classic open-source projects, the Tor Project was never really interested in a huge community of users hacking on the code, rewriting it, producing their own spin-off versions, and modifying it on-the-fly. Instead, the team wanted something that worked, that people could trust (even if they didn't trust the US government or the Tor Project team), and that people would actually use. Although they were eager for people to build new apps on top of Tor, the core design itself was too complex, and relied on by too many people, to be changed or tweaked without substantial discussion and oversight. Scrutiny of Tor is therefore effectively outsourced to a global community of academic and private sector security researchers, and to an information security press for whom the discovery of any tiny new vulnerability in Tor is headline news that can make a young researcher's early career. So in reality, most of those running the infrastructure understand very little about how it actually works.

That's not to say that running a relay isn't a skilled operation—it just takes a set of skills that is different from those required to hack on Tor's load balancing or crypto protocols. As a relay operator, other kinds of knowledge come to the fore. For example, legal knowledge, in particular, the legality of running different kinds of Tor node in your own jurisdiction, has always been of more use to a relay operator than a deep knowledge of cryptography, especially to those starting out.

> Get in touch with the laws of your country. Read, read, read. Understand, understand, understand. And . . . try to have the Tor network growing . . . Depends on your intention—if you, if you don't have any technical background and you just want to help the Tor network, it's very important to know the laws of your country.
>
> Tor relay operator

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

So what do relay operators actually do day to day? To many operators, running a relay is a lot like keeping a bonsai tree—a slow, contemplative practice, tending something that (metaphorically) sits on your windowsill and matures over time. The operators I spoke to viewed their work as a mix of a hobby, charitable work, and public service. They saw it as a practice of cultivation and contribution, like working in a community garden. For those running a host of high-capacity relays with support from an organization, things look rather different—a slicker, more professional sysadmin job. But for many, running a relay itself, much as with any open source infrastructure project, is less a matter of hard technical knowledge and understanding and more something closer to folk magic—the sharing of tacit knowledge between a growing community of maintainers, through guides, mailing lists, and personal experimentation.

> I've begun to realize that running a fast Tor relay is a pretty black art, with a lot of ad-hoc practice. Only a few people know how to do it, and if you just use Linux and Tor out of the box, your relay will likely underperform . . . In the interest of trying to help grow and distribute the network, my ultimate plan is to try to collect all of this lore, use Science to divine out what actually matters, and then write a more succinct blog post about it. However, that is a lot of work. It's also not totally necessary to do all this work, when you can get a pretty good setup with a rough superset of all of the ad-hoc voodoo. This post is thus about that voodoo.
>
> Mike Perry, Tor-relays mailing list, 2010

Once a relay is set up, there are a number of things a novice operator needs to do. They need to maintain good relationships with the internet service provider (ISP) that they are hosting the relay server with, keep on top of bills, keep track of how much the relay is being used, and occasionally engage in a bit of education, explaining to the ISP what Tor is and why they should put up with it. The relay itself needs tending—checking on it to see if it has "fallen over" and stopped working, downloading and applying software updates regularly as they come out, and managing bandwidth, exit policies, and abuse complaints.

Although the so-called *Dark Web* was born far later, people had been misusing Tor since its earliest days. File-sharers were some of Tor's first and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

most enthusiastic early users, exploring the network as a way of countering the backlash from media companies who were working with ISPs to detect people torrenting copyrighted products and to serve them legal notices. One of the first posts on the casual *Tor-talk* mailing list (a general discussion list kept separate from the development work) is from a disgruntled relay operator, who had come home–

> to find a rather unpleasant e-mail sitting in my inbox. It was a DMCA Complaint from the MPAA, for "CHRONICLES OF RIDDICK, THE". I scratched my head for a few minutes, trying to figure out if I had downloaded that movie on my server. I was really quite sure that I hadn't downloaded it, or any movies at all. I wondered if they might have misidentified a legitimate torrent. Then it dawned on me—with the recent talk about BitTorrent over tor, it probably was someone using BitTorrent over tor . . . I'd very much like to continue running a tor server, but I can't afford to do it if I'm going to receive DMCA Takedown notices. Has anyone else had this problem? Any suggestions?
>
> Tor-talk mailing list, 2004

This early relay operator was in fact none other than Anna Shubina, now a well-known security researcher at Dartmouth College.

Tor was always very good, even from an early stage, at combining with other technologies. This was a core part of its design and in fact how the engineers wanted it to spread: if you're busy running, developing, and maintaining a complex infrastructure, it's pretty handy if another group of engineers or another project can integrate it into their much more popular software. However, despite its early links to file-sharing, the movement of some of the BitTorrent community onto Tor was not wamly welcomed. Some BitTorrenters had begun to use the Tor network in its very early days to avoid an ongoing massive backlash against file-sharing by media giants, who were teaming up with ISPs to wield punitive legal takedowns against those copying their movies and albums. This not only caused real issues for relay operators, who became the subject of these complaints, but it also threatened to swamp the young Tor network with more traffic than it could handle.

In the early 2000s, a huge swath of internet services, projects, and applications were being launched—all of which faced problems of abuse.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

In this regard, Tor was little different. In addition to illegally downloading cult Vin Diesel films, a range of other deviant (or at least illegal) uses of Tor have abounded since its earliest days. Given the early user base of techno-libertarians, who, unlike the more recent crypto crowd, believed in the capacity of the internet to democratize access to information, much of this took the form of copyright violations and illegal file-sharing. Some enterprising spammers and trolls had also begun using it to post abusive comments on a range of websites and evade IP bans. As Web 2.0 emerged, based around platforms and user-created content, there was an increasing backlash against Tor from its sister web projects, who were themselves trying to clamp down on users that didn't want to play by their rules.[7]

Early attempts to regulate this focused on the effects on the network—many of these abusive use cases were a pain at the technical level, hogging bandwidth, flooding the network with spammy connections, or getting Tor banned from ISPs and services like Wikipedia. The solutions, therefore, tended to be technical—dominated as the tiny Tor network was at the time by the engineers—with some solutions involving allowing slower relays to join the network in order to limit BitTorrent downloads and open up more capacity, banning email traffic through relays by default, or trying (and failing) to come up with elaborate token-based systems to allow access to abuse-sensitive services like Wikipedia.[8]

This set the tone for much of Tor's early years—viewing misuse as an irritation and an administrative concern, rather than an existential threat. While some early operators bristled at the things their users were doing, the developers reiterated that attracting this kind of dodgy traffic was not only inevitable, it was desirable—growing the user base and helping provide anonymity for the legitimate users of the network.

> [Relay operator 1]: I know that freedom from censorship is a fundamental principle of anonymising systems, but if people wouldn't mind minimising casual [porn]-surfing via Tor, it'll make my life easier.
>
> [Relay operator 2]: Why would I use Tor if I couldn't access porn? . . . Seriously, porn access is the killer app for anonymity solutions. You won't have much of a user base if you disallow access to 'offensive content' . . .

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

[Relay operator 3]: You could identify the servers used to download [porn] and remove them from your exit policy. If bandwidth is a problem, I suggest that you . . . bandwidth limit your node.

[Roger Dingledine]: Yes, this is a perfectly friendly and simple way to disallow exiting to certain sites while still generally allowing outgoing traffic. Clients with a certain destination in mind will automatically look at your exit policy and choose a different exit node.

or-dev mailing list, 2003

Tor wasn't inventing any of these debates itself—they had been well rehearsed in earlier systems, with even Dingledine's master's thesis mentioning the issues with abusive traffic that early remailer systems had been facing.[9] Even these early and relatively minor forms of misuse slowed down Tor's growth, cutting it off from important alliances, deterring relay operators from continuing to support the network, and hurting its ability to link up with other projects. For many sites, especially those like forums, comment sections, Wikis, and Web 2.0 services that rely on user-generated content, Tor thwarted the IP-blocking that was their go-to method for dealing with abuse and spam. These caused a range of practical nuisances to these services, which in the late 2000s were in periods of exponential growth within the West, less dependent on expanding a global market, and selling themselves on user experience. Improving the service for existing users (and thus competing with their rivals) by blocking Tor tended to outweigh encouraging access to small numbers of people for whom these services were blocked.

For many Tor exit relay operators, dealing with this kind of abuse traffic has become a core part of the job of running a relay. Operators walk a delicate line between providing a service and becoming a nuisance—the Tor network infrastructure isn't really separate from the internet and relies on regular internet service providers to allow relays to operate. This means that the grueling task of abuse management falls on the operator.

Lately, more and more, systems are set up to send out notifications if there was some kind of [hacking] attempt like scanning all ports or scanning URLs for like, the typical exploit stuff . . . So when there's filesharing stuff happening, you are required to reply, and that could mean, basically what we do is, is respond and say sorry, we can't identify the customer. So, last time I looked we

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> get a thousand DMCA complaints every day . . . Um, but a lot of ISPs don't like that workload, when they see a lot of these emails. And they are not really happy about putting you in the abuse contact, because they don't know how you will deal with the more severe cases.
>
> Tor core contributor

While a thousand complaints per day isn't the norm for any but the largest relay operators, responding to legal complaints makes up much of the administrative work of running a Tor relay. It involves replying to these complaints with a stock response saying that customer data isn't held for the offending users, and often smoothing things over with the internet service providers, who tend to take a dim view of any service that generates vast amounts of work for them.

These are practices of system administration rather than engineering or design, but they still come with their own tough decisions to make. First off, an operator needs to decide what kind of relay they're going to run—a non-exit relay, which the Tor network will assign as either a guard relay (which manages the first connection to the network) or a middle relay (which provides the middle hop, simply funneling data between two other nodes in the network), or alternatively the more legally complicated exit relay (which makes the final connection to whatever website or service the Tor user is trying to access).

Then, relay operators, like any administrator or service provider, have to decide on the "policies" that they will enforce in their service—what they will allow their users to do. Censorship is, in theory, an absolute taboo in the relay community—freedom of information is a core value of both the wider Tor community and the Project itself. But in fact, almost all relay operators censor their relay traffic. Tor embeds a variety of ways of doing this. Although operators can't censor particular topics (as most users encrypt the content of their communications), they do have a degree of control over what passes through their relay. For example, they're able to ban traffic based on the communications ports that computers use to separate different kinds of traffic, like email or messaging apps, from one another. As one might expect, this is generally framed not as censorship or policing the network, but through the language of administration and network health—and of privacy itself,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

with operators being allowed to choose to contribute to Tor only in ways in which they themselves feel comfortable.

So, for example, due to the preponderance of email spam and the existence of a wide variety of sound anonymous remailer systems, many relay operators don't allow email traffic through their relay at all. This means that some kinds of traffic get better usability and privacy from the network than others—in the case of email, the operators generally assume that slower systems provide a better alternative to the low-latency, real-time anonymity of the Tor network, as people are rarely desperate to receive email at sub-second timescales. The default policies that come with a relay as standard are, in the Tor Project's own words, fairly restrictive, prohibiting all email and internet relay chat signals (as these can be used to control botnets), censoring the ports that computers use by default for those kinds of traffic. In the 2004 USENIX paper, they credit these defaults as the reason that the project faced "no recorded abuse so far." As I discuss in Chapter 8, this wouldn't stay the case for long.[10]

The relay network, growing from an initial group of people known to the Tor Project developers and the cypherpunks, developed slowly into something like an autonomous self-organizing community over the next several years. With remarkably little central coordination other than a dedicated mailing list for sharing ideas, tips, and discussions, it grew into a global community of contributors. As things progressed, a range of organizations sprang up from the community explicitly to serve the Tor network. Some of these were formal companies or NGOs, like the Calyx Institute (which operates one of the network's longest-running relays, since 2007), while others were more like members clubs or professional organizations, such as the Zwiebelfreunde group, which operated in the mode of a traditional German professional practice association.[11]

The relay network began to grow its own cast of characters and personalities—people often known for other work in the hacker scene, but who became the "voice" and public face of the relays. As Tor began to seep through the culture of the hacker underground, the people who attended these huge annual celebrations of hacker life—working day jobs in university computing departments, public libraries, and internet service

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

providers—would set up high-capacity relays at their work or on private servers when they had finally got home, showered, and tipped an avalanche of stickers and badges out of their luggage. Others, like Brass Horn, would try to innovate the network in other ways, like setting up their own ISP.

Part of Tor's strength is that anyone with the capacity to set up a server can contribute, no matter their motivations. This allows for collective action without the need for shared political allegiances, and a large, ideologically diverse community of contributors. Despite sharing practices through wikis, mailing lists, and online chat channel discussions, and meeting up for annual hacker conventions, the wider relay operator community has been rather atomized for much of Tor's history—more a collective of individuals and organizations than a coherent group. Whatever "community" of relay operators exists has, until recent years, been a fairly loose-knit network composed of individuals with their own motivations, political opinions, and levels of technical engagement.

> I think [Tor works] probably because it's easy to work together. We don't actually have to work together! The Tor Project has made it so simple to start a relay and just run it, and not actually interact with anyone . . . they've made it so easy to, to act like a big community when actually, we're not really, I think we might be a bunch of individuals . . . We don't have to co-operate with each other, apart from running the same software.
>
> Relay operator

Although this autonomous decentralized community seems like an anarcho-libertarian dream—a genuine and rare example of coordinated autonomous productive activity—in fact a lot of work goes into herding this infrastructure into a secure and productive state. A truism of IT engineering is that computer systems "like" to centralize. In practice, the Tor network design requires constant maintenance and upkeep to *stay* decentralized. Some of these flows are driven by economic forces, as relay operators try to get the best and cheapest deal for hosting within a dwindling market of internet service providers. As fewer and fewer ISPs agree to serve Tor relay traffic, the options have become more limited, and operators have tended to cluster around a small number of well-known providers. There is also a geographic

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

component to this—some jurisdictions are far friendlier to Tor relay operators than others, legal situations differ from country to country, and dealing with a hosting provider is generally easier if you speak the same language.

When combined, this can lead to some rather perverse effects. Although relay operators themselves might be spread around the world, they rarely run their relays off their home internet connection, and so the server itself might well be in a different country. For some time, an ISP in France called OVH was a top candidate for new operators looking to run a high-capacity relay on a budget. This meant that at one point, a double-digit percentage of the network's relays were run from a handful of hosting providers.[12] Given how ISPs manage their servers, it's not impossible that a substantial proportion of the world's Tor traffic was traveling through a handful of server rooms in the south of France. This may be efficient, but it is not particularly secure, and so the relay community now spends a great deal of time sharing practices and strategizing among themselves, mostly through a shared mailing list and semi-regular in-person meet-ups.

Other forms of relay diversity became important as well as the network grew. The network needed relays hosted on many different operating systems—not just different versions of Windows and MacOS, but a variety of flavors of Linux and more arcane systems like FreeBSD—so that if a deep-level exploit or vulnerability were found in Windows, for example, it wouldn't compromise the whole network at once.

As the relay network boomed, the idea of Tor spread through hacker conferences, mailing lists, and press coverage and an incredible group of people began to come together. As I interviewed a selection of relay operators from around the world, it struck me that the humans oiling the gears of the Tor network looked a lot like the ragtag association of different people and politics long imagined in techno-utopian visions of a future internet. Some of the people who spoke to me were passionate internet freedom activists, others strong feminists, while a handful seemed to hold far-right sympathies and spoke to me throughout the interview about their views on immigration and surveillance by the "New World Order." The relay network appeared to be something approaching the idealized social structures of radical libertarianism or some forms of anarchism—a centerless mass of individuals

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

who nonetheless managed to come together in communal action. And this is no accident.

The relay network began as something approaching a designed community. The structure itself, which was decided and set into place by the design choices made by the engineers, predisposed particular structural forms and relationships between the people in the network. This had important shaping effects on its culture. This culture itself was designed to have security properties, which would transfer from the humans running the network and the links between them to the relays, and from them to Tor and the people using it. The decentralized social formations of the network would create a space in which it was hard to collude between large parts of the network for the purposes of spying on relays or trying to exert power on the core Tor organization—not least because many of these groups simply would not work with one another.

The diversity of people and places represented in the network also made it easier to sell Tor in different ways to different countries and institutions. With no real shared culture or set of political beliefs uniting the network, this would maximize the number of people who felt they could contribute, allowing them to find their own meaning in the network and adapt their arguments to suit their own circumstances. Some might make the case for Tor to a human rights activist on the basis of digital freedom and human rights, while to certain politicians might paint it as a libertarian, small-state technology. Still others would focus on Tor as a tool for exposing financial corruption, or aiding police investigations. Others could make more technical arguments. And this diversity helped the operator's own safety—a government wouldn't be able to infer anything about someone's motives for running a relay.

This blurring between the cultural properties of the relay community and the security properties of the network was designed by the engineers, but the network quickly took on a life of its own. It grew in ways that would challenge Tor's developers at key points throughout its history, and itself changed and ruptured as Tor's own place in the wider world of internet technologies shifted. Despite the atomized nature of the operator community, many of the relay operators I interviewed *did* feel part of a shared culture that had

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

grown up around them, emerging from the day-to-day work of supporting the Tor network and incorporating a deep set of beliefs about security, privacy, and resistance to state surveillance.

As I interviewed them, it became clear that a second privacy world had indeed emerged in Tor—one that was quite different from the *engineer* world of the core developers and far more rooted in the scrappy hacker underground. It had a range of features beyond those "designed in" to the network through the structures laid out in its design documents. Growing out of the relay network, as it spread across the globe, was what I began to call the world of the *maintainers*. In the daily practice of maintaining a relay, coupled with the shared elements of a (very diverse) global hacker culture and the atomized structure of the network, a distinctive culture was forming. Its adherents were the digital equivalents of the janitors, administrators, and railway signal operators who kept the infrastructure running safely. At the heart of the *maintainer world* was a particular vision of privacy that could be roughly summarized in a single phrase: *privacy as a service*.

> I think for someone who's doing it in the spare time or hobby, it is more like "ohh, this is spooky, this sounds nerdy, let's give it a try!" and for me as a technician, it's like, OK, I have the possibility to provide services to people which have restricted internet. I think for, uh, the free-time IT nerds it's some play stuff and if you're kind of a professional, it's like, bringing out a service. That's my opinion.
>
> Tor relay operator

From the point of view of a relay operator, usually an IT hobbyist or someone working a tech job rather than a naval scientist with a degree in cryptographic engineering, Tor wasn't just words and structures in a design document or repositories full of code—it was a hard and unruly material thing that exists in the world. As they tended and maintained their relay, they saw the lives of real people flow through it—for better and for worse. This brought into sharp focus all the ways in which design elements—decentralization, openness, security—had to be implemented and maintained on the ground, reproduced through daily practice and often frustrating work. To them, the structure was only half the battle; they had to make it a reality.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

This idea crystallizing in the relay community, of *privacy as a service*, stood in stark contrast to the disruptive technopolitics of Tor's designers and their visions of rewriting the world with code. Where the engineer world saw Tor as an attempt to redraw the structures of informational power online, the *maintainer world* was more agnostic about Tor's relationship to power, understanding privacy as a service provided to users who engaged in political action themselves. They were immersed in the material reality of the structures that the engineers were trying to make—keeping the messy nuts and bolts oiled and in place. And the world arising from thinking of privacy as a service was anxious to "neutralize" the politics of the work as much as possible.

The practices and rhythms of running a Tor relay led many of the operators to bristle at the idea of Tor having its own politics at all. Some of this was a practical reaction to the political diversity of the relay community. Many relay operators in the Global South, while interested in promoting internet freedoms, were not necessarily doing so with a goal of underwriting US global soft power. The hacker anthropologist and digital ethnographer Gabriella Coleman describes a similar "political agnosticism" in the open source community as an expression of the interaction between the liberal values and technical practices of hacker culture.[13]

When applied to the technology itself, this often came out in rather odd statements—Tor as a tool, with no intrinsic meaning of its own. Again and again within my interviews with the relay community, the same phrases kept coming up:

> It's like, [*sighs*] it's like having a knife—with a knife you can cut an apple and with a knife you can kill a man . . . so the Tor network is just a knife which is laying on the table without anyone touching it. That's my opinion.
>
> Tor relay operator

> Tor is a pen and paper. As with anything in this world, people are the problem, not the technology. Any technological constraint is doomed to slip into censorship.
>
> Onion Service developer and relay operator

On the face of it, this couldn't be further from the engineer world, in which Tor was a radical, transformative intervention in structural politics.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

But rather than dismiss this idea out of hand, it's worth engaging with it deeper in its own terms. The distaste, I found, was often with the *aesthetics* of political organization, rather than with politics per se. Within this agnostic view of Tor's politics lay a common commitment to deeply political values: the vision of a privacy-focused internet where the flow of information, capital, and communication could proceed without surveillance or censorship. These were core to the "hacker ethic"—though here expressed through infrastructural labor, framed around providing services rather than creative breaking.

This aligned with the techno-libertarian desire of the engineer world to reimagine the internet infrastructure, but it focused less on the details of technopower. Instead, their job, as they saw it, was to unravel the legal and administrative knots that were harming the network "on the ground." As custodians of the hardware, they were focused on preserving this infrastructure as neutral—as a space of anti-power. They saw Tor itself as having a responsibility not to weigh its own power in behind one side or another in political conflicts and movements, lest it start to become a technology of control in its own right.

> I think that's a valid argument against Tor. That no matter how much you try to educate people to be able to use it, ultimately you are supporting the power structures. Because only they can understand and teach it. It's like . . . you have all these organisations that teach other organisations about encryption and how to use it. But someone is paying them, right? Someone is deciding what kind of opposition groups they will teach. They can make the decision themselves, maybe. Um, but ultimately someone has to make that very political decision. Of who will be trained to be able to use that. And in that sense, then Tor becomes a weapon against those that just don't know how to use it, right?
>
> Tor core contributor

This idea—of technology not as neutral, but as with political power to be *neutralized*—has a long history in hacker spaces. This political agnosticism is sometimes rather unfairly parodied as naive computer scientists not realizing the politics embedded in their products. But far from seeing technology as neutral, if anything, these classic forms of hacker culture saw technology as dangerously political, drenched in a complex mess of law, values, and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

debates that make for dangerous distractions from the "real" technical work. But, as has been noted by many, this reluctance to deal with "politics" has been used as an excuse to allow bigotry, bullying, and abuse within hacker communities.[14]

The moral queasiness that arose from the work of running a Tor relay itself acted as a powerful antidote to getting too "political"—condemning or praising one type of traffic or user over another meant wading into a swamp of harm and abuse that wasn't always pretty or easily defensible. It also made Tor an easier sell to domestic internet service providers, local police, and government in the countries in which relay operators worked and lived. When the political values of Tor could be neutralized, it could be sold as a security technology, an anti-corruption project, or an academic experiment rather than a crusading Western human rights struggle. Even in liberal democracies with a nominal commitment to human rights, this proved useful—allowing computer science departments, libraries, and data centers to become a home for high-bandwidth Tor relays in the name of "science" rather than encouraging risk-averse university administrators to sign off on global resistance projects.

The maintainer world would continue as a strong voice against attempts on the part of the organization to decry or promote particular use cases, legal or illegal, or to claim that Tor itself represented any specific set of values outside a neutral service for protecting data in transit. By constructing themselves as apolitical actors, they shifted the moral character of the network onto the users, allowing them to contribute without feeling responsible for the traffic which their relay served.

> I think most of us believe that we want to provide the tools so others can exercise their powers and their influences. People that understand society better, maybe. And we are just the infrastructure providers. Right? I think that's a notion that a lot of hackers have, is that ultimately they don't want the political influence, they just want to provide the infrastructure. For democratisation.
>
> Tor core contributor

While the relay operators were busy maintaining the network's physical infrastructure, a range of other maintenance tasks were spilling out of the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

technology at a rapid pace as the work of the developers began to change. Although Tor remained a focus for cryptographic development, research, and experimentation, maintaining the code became a top priority. The older the codebase became, the more likely it was that an attacker would compromise the network and its users not through a clever attack on the Tor design, but through a software bug in an aging software module. Though the core team kept building new features and capabilities, much of their job was just keeping the code running, trying to make things faster and more stable, and the eternal grind of finding and fixing bugs. The maintainer world spread beyond the relays, to the many new programmers and developers joining the project, whose work wasn't on design or crypto, but on maintaining the software.

> For some it's impact—they want to change the world. For others its challenge. Personally, I don't lean towards those. My interest is in our community and doing quality work. The magnitude of impact isn't a prime motivator for me—I don't care overly much if my work greatly changes the world or not. Rather, I just care that the things I do are done well. I suppose that's why I lean towards support and infrastructure roles.
>
> Tor core developer

From relay operation, to code maintenance, to lobbying internet service providers, to administration, the maintainers fought against the entropy that constantly threatened to degrade the Tor network's core infrastructure. The maintainers and the engineers rubbed along very well for much of Tor's history—both were focused on the infrastructure and recognized that they needed one another. Dingledine was always particularly talented at bringing together the "neutralized" politics of the infrastructure and the structural politics of the design, able to talk as easily to the cryptographers and anonymity engineers of the Privacy Enhancing Technology Symposium as to the libertarian hackers of the Chaos Computer Club (with which there was already a substantial overlap in membership). But for Tor to grow further, it would need more than just a design and an infrastructure—it would need money, users, and organization. And that meant that it would have to engage in the world of politics.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

6 THE ONION GROWS ROOTS

Once the relay network had begun to grow, Tor's roots spread out in other directions as well. For the next several years, Tor would grow its own institutions and link up with others—developing a dense network of connections to the hacker underground, policymakers, lawyers, campaigners, and other groups. The internet was growing alongside Tor, spreading around the world, pushing into politics, and upending entire industries. Although many see the internet as having changed the world, it would be more accurate to say that they changed each other—the cultures, institutions, and power relations of the world affected the ways in which internet technologies developed as much as they themselves were transformed. The internet's infrastructures were also growing a set of institutions of their own—institutions with their own cultures, values, and ideas.

After Tor's initial release and Roger Dingledine's tours of the conference circuit in its first year of life, Tor was given a home by the Electronic Frontier Foundation (EFF), an American nonprofit that began funding Tor in 2004. EFF has long been one of the most prominent global organizations fighting for digital rights. A US nonprofit staffed by technologists, lawyers, researchers, and advocates, it was originally formed in 1990 by a group of cypherpunks, many of whom are now familiar parts of internet history. Its foundations, like many parts of Tor's history, are rooted in a series of conflicts and accommodations between hacker cultures and the repressive force of the state—and are also deeply strange.

The hacker underground, evolving through bulletin boards and small communities across the 1970s and 1980s, had been developing a distinct

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

culture. The values and ethics of these communities crystallized in a document known as the *Hacker Manifesto*, published on hacker bulletin boards in 1986.[1] Its author, Loyd Blankenship, a member of a number of hacker groups at the time, set out a utopian vision of the internet in which the vast, interconnected spaces of an online world would open up systems of power to new kinds of disruption—a place where the technical skills of individuals would overcome the static structures of oppression. Blankenship, later working at a company that made tabletop role-playing games, was targeted by the FBI, which believed that he had hacked into BellSouth's computer systems. This provoked an immediate backlash from the hacker scene and the proto-cypherpunks of the Bay Area.[2]

A group comprising some odd characters—including John Perry Barlow of the Grateful Dead (who had written his own manifesto called *A Declaration of the Independence of Cyberspace*), Apple cofounder Steve Wozniak, and some libertarian entrepreneurs in the computer industry—took the FBI to court, successfully establishing the legal principle that law enforcement must obtain a warrant to access emails in the same way that it must to access private homes. They also worked with some of those targeted in a separate "hacker crackdown" called Operation Sundevil.[3] Despite the scrappy and eccentric nature of some of the founders, they put together a professional advocacy group—the Electronic Frontier Foundation. Over the years, EFF has focused on tech policy advocacy and challenging threats to encryption and overreach in online surveillance, engaging in a range of (often US-focused) legal battles with many prominent victories to its name. It was one of the main combatants in the Crypto Wars—while onion routing was taking form at the NRL, EFF was challenging in US courts the classification of encryption technologies as military exports.[4]

Throughout the 2000s, the wider landscape of digital rights was changing.[5] In few places was this change clearer than in EFF's continuing rise to prominence. The last (and sometimes first) line of resort for people being victimized by overzealous digital law enforcement, EFF became involved in many of the high-profile digital security cases of the time, building links to the hacker underground and the cypherpunk movement. Shari Steele, a longtime digital rights advocate who had led EFF's legal efforts and shaped it into a

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

professionalized organization through the 1990s, became the executive director of EFF in 2000. As just one of a range of new initiatives she led, Steele extended the nonprofit's work to include its own technology program. In 2004, EFF hired its first socially responsible tech director, Tim Pozar, who would lead a four-person team tasked with developing a technical program within the organization to work on "technologies that advance free speech and privacy."

EFF's culture was rather different than that of the technical scene, and by the early 2000s, when Tor was entering the world, it was much more professional. The organization was composed of mostly lawyers, policy professionals, lobbyists, commentators, and full-time activists, distinct from the crusty libertarians in the hacker underground. It was part of the wider digital freedom social movement, engaged in legal action and public campaigns around net neutrality and other major battles erupting as the shape of the new internet industry was being formed by legislators, regulators, and law enforcement. These people could put together a slide deck, pitch million-dollar grant bids, and get meetings with high-level politicians and funders. And they saw privacy primarily as a human right.

Although the glimmerings of more activist ideas were always part of Tor—visible in the radicalism of the cypherpunks and their conflicts with government, and in the protests and tense political debates raging in the hacker underground—the people involved in the Tor community at this stage generally chafed at the idea of privacy as a *social movement*. The engineer world was distrustful of policy and legal debates, preferring to change the world through technical fixes, and their limited and unstable funding from government was dependent on grants for scientific research, not activism. The maintainer world that was emerging saw itself even less as a home for activists, committed as it was to a "broad church" community that could attract participants from all political stripes. But the Tor Project still needed money to support the development work and was desperate to move from the "feast-and-famine" cycle of research grants to a stable funding stream, especially as it broadened in scope from conceptual anonymity engineering to maintaining a large-scale network for general use.

Although Dingledine and Mathewson were great developers and good spokespeople, their initial efforts to get money from the hacker underground

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

conventions were less than successful. So they partnered with EFF. Steele, who would go on to champion Tor within the organization, agreed to bring the baby Tor network under EFF's umbrella, providing a small amount of funding and an institutional home for a year.

Tor was the first major technology project that EFF sponsored. Although this new funding opened up room for Tor to grow, Dingledine, operating under the name Moria Research Labs, continued to consult on Tor via the NRL. Tor existed under EFF's umbrella for a year as promised, but the intention was never for it to be a long-term home, but rather a place for Tor to develop its own sources of funding. While in EFF, the young Tor team became a slightly slicker operation, with assistance in creating a website and other new aspects of the project. EFF's support connected the Tor team with activists and journalists, who, through organizations like Reporters Without Borders, Human Rights Watch, and Amnesty International, trained front-line workers to use the Tor network for secure communications.

However, the end of the year's sponsorship coincided with a funding dry spell for EFF in 2006, and the money for Tor ran out. Little tangible progress was made toward a stable financial life for Tor of its own. Further efforts to find funding in the hacker scene had still found only limited success—though the team was spreading awareness and attracting an increasing wave of volunteers and excitement, this rarely seemed to translate into financial support. Tor was still largely dependent on funding from the US Navy through direct grants supporting Dingledine and Mathewson as core developers; securing a long-term future for Tor still required finding sustainable funding. It was at this point that Shava Nerad arrived at the scene.

Nerad, a long-standing member of the digital rights community around MIT, had been working in licensed entertainment marketing for major corporations as well as in politics. She was between jobs in 2005 and rather different from the people who had been working on Tor in its early years. Although she had heard about Tor through the information security grapevine, at the time it still very much had the image of a technical product with a niche, hackery audience of security industry professionals. Some of her friends in the corporate tech start-up scene were working on a pitch to Tor to help turn it into a company, and they explained to her that many of

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the users Tor was courting were the same activists with whom she had been working for the past decade.

But this slicker crew of entrepreneurs had a hard time making the pitch to Dingledine, as they had a very different understanding of what made a technology project successful. Although both they and the Tor developers wanted to turn Tor into supported software, they—marketing professionals—couldn't see the potential profit in Tor's mission to provide free services to users, and argued that only a small amount of cash would be needed to fund ongoing user support. Dingledine, already watching the mailing lists fill to the brim with basic questions from Tor's early users, foresaw a future in which half of his and Mathewson's time would be spent simply doing tech support. They would need real money for development and primary cryptographic research.

Nerad switched things up—although she had come with the corporate team, she saw the argument Dingledine was making and agreed. The pitch was dead in the water—as she made clear, Tor needed money for highly skilled cryptographers and the technical demands of the project meant that it would never make for a profitable business model. Impressed, Dingledine introduced Nerad to Mathewson over a meal at a local Italian bar. Nerad, who had a long track record of successful funding bids, explained to them why their pitch for the network wasn't landing with funders. They invited her onto to the team and she agreed, under the condition that she be the executive director and they let her lead the organizational side. They would then be free to focus on the tech.

Nerad's first contribution was to insist that they incorporate as a 501(c)(3) nonprofit organization in the United States. This would give the team substantial protection if foreign states came after them, and, as she knew well, the fractious national political environment would work to their advantage, allowing them to play their critics off against each other and get funding from a more diverse range of interests—especially with an expert like her on board. Somewhat reluctantly, Dingledine and Mathewson agreed not to speak to the press, allowing Nerad (who knew how Tor would be received by a media desperate for controversy) to take the lead on Tor's public relations efforts.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Nerad came on as executive director, with Tor continuing to work as an unincorporated open source foundation for the rest of 2005 until it incorporated in 2006. This let them lay the groundwork to get their initial grants in place. Nerad was able to tap into what at the time was a rapidly expanding source of public funding for journalists, human rights workers, and pro-democracy projects, where grants were orders of magnitude larger than those for security research or open-source projects.

The funding that Tor developed over the next few years was split between three streams, each from its own context: computer science, cybersecurity, and politics. The first two of these streams were technical—one for developing primary computer technologies and conceptual innovations, and the second for contributing to security and cryptographic research that could be incorporated into other technologies. But of equal importance here was the third stream: the political funding.

The International Broadcasting Bureau (IBB), which also runs programs such as Voice of America, was the main funder of Tor for some years, and itself has an interesting history that highlights some of the tensions within Tor's political mission. Its own roots are deeply linked to the twentieth-century history of communication networks as a means of shaping global power. Radio Free Europe was founded as a CIA front organization at the start of the Cold War in 1949 by Allen Dulles, later the head of the agency, to distribute pro-democracy propaganda in Soviet Europe. Successive radio outfits—Radio Liberty, which targeted Russia, and Radio Free Asia in the 1990s would echo this mission in other regions of the world, mixing broad cultural programming with specific disinformation campaigns to support operations on the ground. This tactic—countering authoritarian regimes through propaganda and promoting Western cultural ideas—came to be known as a *soft power* strategy.[6] These information warfare tactics weren't limited to the United States; culture is a core weapon in the arsenal of the modern state. But during the Cold War, this became a key tactic in the conflict between Russia and the United States—an ideological and cultural battle that raged alongside the *hard* conflicts of proxy wars, nuclear posturing, trade embargoes, and espionage.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The CIA would covertly fund Radio Free Europe until the early 1970s. After the collapse of the Soviet Union, as the 1990s progressed and the United States adapted its soft power efforts to a new geopolitical era, the Clinton Administration established the Broadcasting Board of Governors (BBG) to oversee a range of media projects, taking over Radio Free Europe, Radio Liberty, and Voice of America. This also involved the creation of the IBB, a technical outfit to oversee the practical and infrastructural aspects of the BBG's programs.[7] This was considerably more complex than simply running day-to-day show operations and technical support, but involved establishing broadcasting infrastructure that could beam these radio programs into countries that were eager to jam them. Much like Tor's efforts to counter infrastructural power, the IBB was setting up its own anti-jamming antennas and educating people around the world on how to use them—a prologue to its support of Tor.

In the mid-2000s, in many of the countries in which the US had been running soft power campaigns through newspapers and shortwave radio (such as Radio Free Asia), internet use was beginning to displace these older formats and the US-backed organizations running these campaigns were eager to "future-proof" themselves against the decline in traditional media.[8] As the so-called "Great Firewall of China" (a series of censorship technologies that cut off Chinese citizens from large parts of the Western web) was being built, Tor was able to pitch itself as a way to get around this. Simson Garfinkel, a long-standing computer scientist, technology historian, and privacy researcher, had mentioned Dingledine and the Tor Project to the IBB and negotiations began in November 2005, just as the funding from EFF was coming to an end. The funding from the IBB came through in 2006, initially totaling around a quarter of a million dollars per year, and allowed the Tor Project to resume paying its staff—including Nerad and Mathewson.

This sparked off further sources of more politically oriented funding for Tor. At the Workshop for the Economics of Information Security in June 2006, held in Cambridge, UK, Dingledine had presented his "Anonymity Loves Company" paper detailing Tor's radical privacy design. A member of the audience—veteran cypherpunk and privacy scholar Bruce Schneier—was

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

impressed by the talk. Schneier had been asked by the Omidyar Network (an organization started by the founder of eBay that promotes capitalist free markets as a tool of social good around the world) to look out for potential digital privacy and anti-censorship projects that might be able to use grant funding. After the workshop, Schneier helped to facilitate a $40,000 grant from Omidyar to Tor, providing the push for them to incorporate as a 501(c)3 organization, with Shari Steele from EFF acting as a sponsor. This eventually led to further funding from Internews later in 2006.[9]

These other sources of funding allowed Tor development to spread beyond the NRL-funded engineering work to new technologies, education and outreach programs, and to improvements to Tor's speed and usability. Although much has been made of the shadowy forces of US soft power funding the Tor Project, there is no evidence that this has ever made Tor less secure for its users. Instead, Tor's funding has generally pushed it toward a greater focus on making it faster and more usable for users around the world, and on circumventing censorship. Tor's multiple priorities—conducting primary scientific research, managing a technical product, and seeking to change the world all at once—had not always been easy to manage within EFF, and that tension was partly why Tor budded off into its own organization.

As Tor laid these foundations, the structure of a more official Tor Project began to evolve from a small open source tech project to something closer to a professionalized NGO. Dingledine and Mathewson remained as the two lead developers and the core of the team, with Syverson continuing to work on onion routing (and attacks against it) with his team at the NRL. Tor, as well as many other open source organizations at the time, began to institutionalize, appointing a board of directors to steer the project, a group that included a number of old crypto characters including Ian Goldberg, Rebecca McKinnon, Wendy Seltzer, and Fred von Lohmann.

Although not tasked with development work, the new leadership also helped steer Tor's technologies in a new direction. Dingledine and Mathewson were at the time focused on improving Tor's speed and security, but its board of directors began to push for usability in other ways—especially in making Tor simpler and more appealing for non-technical users. This had been an obstacle to broader funding—the first results for web searches for

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Tor were entirely technical and security-focused. Although not yet associated with crime, it was seen as more the purview of hackers and governments than everyday users or human rights activists. Nerad was crucial in helping to reframe Tor to support its new avenues of funding. Taking a trip to Washington, DC, she stopped at several human rights organizations—including Amnesty International's US headquarters, which she knew from her previous work used Tor on the ground in their frontline operations. Rather than ask for funding (which would have been unlikely given Tor's image), Nerad instead asked them for press—to mention in blogs and news stories if they had used Tor. This public relations campaign began to quickly change Tor's reputation as a high-security hacker technology—instead of arguments at crypto conferences, a search for Tor now returned endorsements from major human rights organizations.

After Nerad stepped down from her role due to ill health in the aftermath of a serious car accident, Andrew Lewman, an ornithologist and computer hobbyist who became a tech start-up-and finance entrepreneur in the late 1990s, joined as the new executive director in 2008. Lewman acted as the public face of Tor to the media and worked to scale up the organization, carrying forward the foundational work done by Nerad. He had been a volunteer since 2003, when he had helped with the website, but now brought an entrepreneurial energy to Tor and steered it into something between an open source tech foundation and a disruptive start-up.

Over this period, Tor stepped into the ecosystem of internet technologies around the world. Its engineers had built it to be compatible and interface with other technical projects, and this proved irresistible to many in the hacker community who wanted to embed it into their own technologies or build new features on top. But despite Tor's image as a technical network, much of its history has happened in the flesh, and the different worlds of Tor have generally claimed a home in their own physical spaces.

For the engineer world, Tor was a research program as well as a disruptive innovation, and thus many of the technical advances were first birthed in academic conferences like the Privacy Enhancing Technology Symposium (PETS), where both the Tor developers themselves and cryptographers around the world would present their attempts to break Tor and devise novel

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

improvements. Complementing this, both the engineer and maintainer worlds had strong cultural connections to the underground hacker scene in its various iterations. Those ties were only deepened by the ease of running a Tor relay—a fun beginner computing project for a newbie hacker, a way for established hackers to give back to the community, or a bona fide side gig with a hint of danger for some IT professionals. The scrappier world of the relay operators had little interest in the theoretical papers and lectures at PETS, but had their own, boozier alternative sites in the form of hacker conferences. As the relay network grew, and more people began to use Tor, this world (represented in the cultures of tech through the *maintainers*) began to play a greater role in shaping Tor's cultural identity.

By 2017, when I was trawling around for interviewees, the Chaos Computer Club (CCC) had been home for some time to a regular Tor Project stall (as well as stalls for its archipelago of sister organizations). Most years, Tor developers gave talks to an audience of hackers, techies, and activists from around the world, many of whom had no formal links to the organization but were Tor relay operators in their spare time. The broader hacker underground didn't contribute only relay operators either—a wide range of people helped the project in different ways. More technical volunteers started their own little projects, hacking on bits of Tor, adding on their own services and sometimes entirely novel features that would be incorporated into the code. Some would begin to volunteer their time to the Tor Project on a more regular basis, slowly becoming part of the core community, giving trainings and talks around the world promoting Tor to new groups of users.

Many of these side projects would become vital parts of the Tor ecosystem, and their maintainers core to the Tor community, such as the Metrics project—initially developed by Karsten Loesing (who started with Tor as a Google-sponsored summer intern but became a core developer and beloved member of the community), and later by Ian Learmonth. Their project gathered minimal data from the relays about how many people were using Tor, and a best guess at their origin country—something that would become crucial in both managing the flow and performance of the Tor network, and in selling Tor as a technology of liberation in the future. A busy and growing scene began to emerge—of developer meetings over tapas in sunny cities, a

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

raucous set of instant messaging channels where the developers would hang out in the evenings, and a raging torrent of discussion, argument, and technical work on the project's ballooning series of mailing lists.

It was at the CCC that Tor formed its first tentative connection with Wikileaks. Wikileaks fits oddly into this story, reappearing periodically throughout Tor's life like a dark comet, often heralding a sea change in Tor's place in the world. Founded in 2006, the idea behind Wikileaks was for it to become something like an activist Eternity Service or Free Haven, hosting secret documents leaked from diplomats, militaries, and spies in a network of servers that couldn't be easily taken down.[10] Its founder, Julian Assange, had been a prominent cypherpunk who contributed to the mailing list in the 1990s when Wikileaks' link with Tor had been at its height, though Assange was never involved in onion routing. Wikileaks shared some aspects (including occasionally personnel) with other digital rights NGOs but was less interested in corporate sponsorship and community-building than in punchy, demonstrative action and making headlines. Particularly in its early days, Wikileaks was not a monolithic organization, and many who joined the project (and did a lot of the work) were motivated by quite diverse political views. But throughout, Assange generally remained focused on opposing what he saw as a rampaging United States using the internet to discipline the world rather than as a utopian vision of technology. As time went on and the organization became more centralized around Assange and his politics, it became increasingly focused on opposing US digital power.[11]

At this point, Wikileaks was already beginning to play an important part in Tor's story. If an ally of Tor, Assange had some odd ways of showing it. In 2010, Wikileaks received its first big scoop of documents—ironically, given its own similarities to the vision and design of Free Haven—by abusing the Tor network (or so they claimed). Wikileaks's source allegedly set up a Tor relay and spied on the traffic that flowed through it, capturing and then releasing vast reams of sensitive documents.[12] As the media reported it at the time, diplomatic embassies around the world, frustrated with restrictive rules banning the use of regular email, had begun to use Tor to send cables. But many of them didn't encrypt the content of their messages by default, so they could be read as they passed through the relays of the Tor network—and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

thousands were captured by a source who then leaked them to Wikileaks. In fact, this story may well be apocryphal. A malicious exit relay would have been able to see only a tiny amount of the traffic flowing over the Tor network—getting the enormous numbers of cables that Wikileaks released by this method would be nearly impossible. It would appear far more credible that a less technical method was used—for example, a source with direct access to the cables passing them to Wikileaks. But whatever the mechanism, this kicked off a series of conflicts with law enforcement and with the US government, as security agencies around the world tried to undermine Wikileaks's attempt to create a Free Haven for anti-US leaks.[13]

Although Wikileaks would come under immense government pressure in the 2010s, Tor had been planning for these kinds of battles since its earliest days and had prepared its own defenses. The easiest attacks on Tor don't involve the technology at all; the *social* threats Tor faces are much more dangerous. In particular, Tor (and its user community) has always been deeply worried about being infiltrated by security services. In theory, the CIA, the Russian FSB, the Pakistani ISI, or the Chinese intelligence service could simply kidnap Roger Dingledine or another important member of the project, hand them a flash drive full of cleverly designed malicious code, and compel them to incorporate it into Tor's codebase. Tor's potential adversaries include a range of organizations with massive budgets, advanced intelligence capabilities, and a long history of espionage, infiltration, and disruption targeted at resistance groups. As it became more well established, Tor's community increasingly came to the fore as its first line of defense against—and in a sense, its greatest vulnerability to—state interference. Under the technical design of the Tor protocol and the servers of the relay network lies a social design, a set of community structures aimed to protect the technology from government attacks.

Despite support from the naval cryptographers and the increasing enmeshment of Tor's finances with the US instruments of soft power, the Tor developers were aware that other parts of the US government might see an advantage in using Tor to its own *hard power* ends by forcing developers to install backdoors—as might governments of countries in which Tor was more actively helping activists, journalists, and revolutionaries. In protecting

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the Tor community and its developers from government attacks, the engineers adopted very similar approaches to those that they used to develop and assess Tor's technical design. To an *engineer* view, social factors like friendships, hierarchies, organizational structure, working practices, communication, and social interaction can be understood as patterns of power and information to be arranged in different structures. And a preexisting social structure for this already existed in the cultures of internet infrastructure—the open source movement.

Tor is an open-source project: its code and design discussions are freely accessible to the public. However, it navigates this openness in a rather distinct way. Tor takes some (but not all) traditional open-source software values and turns them into the primary design principles to protect its community. In traditional open-source organizations like Linux or Debian, the openness of the software is a moral imperative—its users and developers believe in cultivating a user base that understands, and can be part of, the design, maintenance, and repair of the technologies they use.[14] They see the internet more as a classic car that you can spend your Saturdays tuning up than a black box that you need to call an engineer from the company to fix. In Tor, openness is instead a security property—for its developers and its users alike.

> You also can't say, oh, here's this binary blob of code we wrote, you know, we're the Navy, trust us, it's great! Um, you need to have it be Open Source, you know, in order for people to know it's OK, and not just Open Source, which is, you know, I guess originally we were probably just thinking that, but, uh, evolving a bit we realised, OK, not just Open Source, but it has to be well-documented, and you have to encourage various researchers to, to pound on it, and then publish anything that they find. And, so, the point is, the idea that you need to have Open Source, freely-available, uh, system design, and code, was in from the very beginning, and . . . that was part and parcel to the security protections you wanted the system to provide.
>
> Tor core developer

Tor extended this openness well beyond what might be expected of a privacy project, putting its source code, financial details, internal bug-tracking and work-tracking systems, design discussions, internal mail, meeting minutes, and the majority of its developers' identities openly on its website.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Although a small number of Tor's core team remained anonymous (using pseudonyms to protect their identities), most lived very open lives, with their names, headshots, and email addresses freely published on the Tor Project website. Tor functioned as the mirror image of a security service—one with openness in place of secrecy.

As the Tor project grew, it attracted more developers—some working for a salary, and many more simply contributing as a labor of love. But the core team was acutely aware of the possibility that law enforcement and spy agencies around the world would try to infiltrate the their community. As imagined, this could involve a hostile agent attempting to become part of the Tor Project, becoming a developer or attaining another position of influence, reporting back secret information and attempting to undermine Tor's technology. The core team thus needed to be careful in managing who contributed to the project, and how. At the same time, however, they also didn't want to impose barriers for new people to join: as a small organization dependent on volunteer labor to survive, Tor got a lot of its power and vibrancy from the constant flow of new people, skills, and ideas into its community.

The team saw radical transparency as an elegant solution to this problem, as having the code be open source allowed them to size up new collaborators and build trust, while allowing those with an interest in Tor the opportunity to follow the development and put forth their own changes to the scrutiny of the community.

> Tor as, as a project is something that's, I think it could not . . . maybe it would exist, but it would not be able to do all the things that it does if it were not for the huge community that we have around it of people that just show up and are aligned with our ideals and believe in what we are doing, and contribute as just a labour of love to the project and to what we are doing. Like, I think, uh, without that we would definitely be much, much weaker and be able to do much less than what we do. So that I think is definitely something that would not be possible if, if we were to have a much more . . . closed and siloed approach to development discussions and whatnot.
>
> Tor developer

Expanding rapidly in the mid-2000s, this growing cluster of volunteers, coming from all sorts of other projects and communities, allowed the Tor

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Project from an early age to punch above its weight as a relatively small organization. Academics at the top of their fields from all over the world were able to contribute to Tor in ways that would have been impossible if the code was not public. An open proposal system meant that ideas from the community were subject to the same scrutiny as the rest of the project's work, making it more likely that malicious changes would be spotted while helping build trust with potential new members.

The second threat facing the developers was their own security. There had long been a perception within the Tor community that there was a risk of external actors compelling individual members to compromise the technology or reveal secret information. Their policy of radical openness dramatically reduced the amount of secret information that was actually held by the organization, in theory making it very obvious if someone had been blackmailed and reducing the damage they could do if they were.

> I would say that . . . I take some precautions. But I think actually the biggest protection is that it is Open Source . . . So, if there was an attempt to, let's say, coerce me into writing a patch that would be malicious or whatever, then that would, I very much hope that would be spotted by somebody [*laughs*] . . . I mean I also hope that I would just not do it. But if there was some way that I was actually coerced into doing it, my feeling is that it's actually [*sighs*] there's not that much value in targeting me, actually? So if somebody did try to target me, that would probably be because *they didn't understand the structure of what I'm doing* . . . I think . . . if I had to sort of keep a lot of things . . . secret in general, or if we were working closed, then it would be a very different kind of threat model.
>
> Tor developer (emphasis added)

As Tor grew, and other internet communities grew along with it, the opinions and chatter of the information security community became particularly important to user adoption. Their reach was wide and growing—what had once been a rather niche profession was now a necessity for every modern organization, company, public service, and government. Spreading and encouraging the use of Tor meant reaching beyond the cypherpunks, to get this growing *infosec* community on board. These security professionals—a mix of frontline researchers, compliance professionals, "red-team" penetration

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

testers who would hack your organization for a fee to show you the holes in your security, "blue-team" defenders whom you'd pay to protect you, and developers building security software or managing your system security as a service—had a subculture of their own. Pipelines and career paths began to spring up from the hacker underground, taking young hackers and giving them routes into lucrative and legitimate work (or at least work which swam with the currents of capitalism and big business instead of against them).[15] As information security became an increasingly vital part of any business, and as company after company fell to leaks and hacks, the status of security professionals grew; once low-level administrator jobs, some were now C-suite executives.

Across the late 2000s and early 2010, a media apparatus had developed around information security, which, along with Tor's prominence as an attractive subject, meant that the discovery of even small vulnerabilities in Tor were now accompanied by significant press attention. Similarly, because of the money that Tor accepted from the US government and its history with the US Naval Research Laboratory, there were large sections of the information security community that instinctively distrusted it, and recommended not using Tor at all. As a result, the Tor community was becoming increasingly anxious about the spread of "FUD," or fear, uncertainty, and doubt.[16]

> I think it's actually more dangerous, all this talk internally in the more technical scenes, the talk about backdoors, about US government funding, about, you cannot trust Tor, um, on various levels and with various intensity. Because I think in the hacker community, there's a growing number of people that don't like Tor anymore. Uh, or never liked it, or are now more vocal about not recommending Tor . . . of course when you're in a technical crowd and you can have these conversations, and you can say, OK there's certain, downsides to this technology, and certain risks that replace other risks . . . But what ends up happening is that people who ask their friends, and they ask their tech guys, and they say no, don't use Tor, then people end up using something that is worse for them. Um, and that's in some respect, for me, more dangerous, to kind of lose this core group, and I think it's the most relevant group because it spreads the knowledge. Um, it's like, if you don't know shit, you will ask the person you know that knows a bit more, and it's like a cascade that will end up

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

somewhere in the hacker scene. And that guy says "oh no, Tor is shit", over a beer or something, and then this will have consequences for users.

Tor core contributor

Tor's transparency helped in part to mitigate this concern, as the security community was brought into the effort of developing and supporting Tor and allowed to scrutinize it in depth. Tor's code was soon reviewed by large numbers of computer security professionals around the world, so users (in theory) didn't need to trust the developers at all. This also turned the natural skepticism of the information security community into an asset: the discovery of a vulnerability in Tor would lead to high-impact research and widespread media reporting, which would further incentivize the community to work on finding and fixing these vulnerabilities, which in turn would further increased the scrutiny of the code. Tor's security would be improved, and its legitimacy bolstered with its users.

The social dynamics "built in" to open-source communities had some useful security properties of their own. The state security actors against which Tor was trying to defend had a long history of skillfully disrupting undesirable activist or resistance groups through stirring up internal conflict and stoking paranoia. This posed a particularly serious threat to Tor, as given the well-trodden history of activist community dynamics, this kind of infighting had the potential to occur even without external provocation. But these efforts often relied on cultivating cabals and secrets within communities—and the transparent information flows of open source in theory prevented an economy of secret information from developing. While other kinds of cliquishness or abuse could (and did) emerge in the Tor community, the open design would, in theory, largely stop this from touching the technology itself.

Uh, so it kind of, it, you know, I mean I think you see this in organizations where they, they keep things secret, not just from the outside world, but because they're keeping things secret from the outside world, they end up being secret from each other too, and it makes it harder for them to, you know, work together smoothly.

Tor core developer

Wikileaks would eventually run afoul of this principle, operating an economy of secret information, like a secret service or spy agency, that led

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

power and paranoia to centralize around Assange. This made both him and the organization itself intensely vulnerable, creating a single point of failure that, when it failed, would fracture the once-diverse community around Wikileaks and tear its work apart.[17]

Open source isn't without its problems—and some of its principles worked in direct opposition to Tor's security design. By fostering a community of user-developers, tinkerers, and hobbyists, open source developed values involving particular ways of dealing with conflict and consensus. The history of open-source projects is famously fraught, with every major decision prompting users to respond with competing versions of the technology, and then voting with their feet. Open source was designed to accommodate these philosophical and technical differences by forking and splintering into sister projects, each embodying their own technical solutions favored by their own communities. But this would be useless for Tor—anonymity loves company, after all, and Tor needed to accommodate a wide and diverse community, not a fractured mess of competitor projects. As Tor grew, the core team became increasingly concerned with avoiding the social dynamics and rifts that they saw tearing apart a range of other technical projects. They needed to manage the Tor community differently than they would a traditional open-source project.

Coordinating debate within a huge and diverse community was difficult. In practice, a set of natural exclusionary mechanisms, particularly the complexity of the Tor technical design and the cryptographic protocols on which it depends, reduced contribution to a manageable level; most people in the community simply didn't understand the crypto-engineering well enough to form an opinion. This also helped maintain a separation between the roles of developer and infrastructure maintainer, as it discouraged relay operators from seizing control of the project or leaving to form splinter groups. Most of the Tor community was happy to let the developers do their own thing, as long as they remained open to expert scrutiny; public debate, then, was often fiercest around the less complex—and less important—areas.

> Um, what colour do we paint the bike shed? [*laughs*] If it's an easy question, everyone has an opinion. If it's a more technical question then less people have an opinion . . . If people have strong opinions about the way it should be done

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> they'll come forward and they'll argue it out, but it'll be a shorter discussion and you'll have less people involved.
>
> Tor core developer

Thus, a kind of tactical bike-shedding" proved an unofficial mechanism of community management, keeping the core technologies from fragmenting.[18]

Fully exposing development and code to the public also brought with it some security risks—especially as the world's best cryptographers were constantly trying to break the technology. Tor's radical openness was never as complete as it might have appeared; not all of Tor's inner workings were actually laid bare to the eyes of the world. Some elements of Tor were kept secret, especially the tools it uses to detect malicious relays in its network, in order to make those tools harder for adversaries to circumvent. While Tor's developers minimized the amount of "security through obscurity" that they employed, sometimes, as is the case for most other security technologies, it was necessary to hide technical aspects of Tor.[19] They also at times had to make pragmatic decisions to protect Tor's users; for example, in the event of a major vulnerability being discovered in Tor, the team in the past practiced "responsible disclosure," waiting until they had a patch ready to fix it before revealing its existence to the community. This is another example of military-academic pragmatism at work—when a serious vulnerability that would take a few months to fix had been revealed, Tor avoided risking the safety of millions of users by not publicizing it until it could be fixed. Maintaining this pragmatic balance, rather than an absolutist approach to openness, required careful judgement and discussion. It too has been subject to some serious criticism, especially from cypherpunks in the wider community who believe in openness as an absolute value, and from conspiracists who see it as evidence of collusion with security services.

> It's a very fine line that we walk. And we basically weigh that decision at every single point and as much as possible, we publish and make available everything up to, but not including whatever information could harm the Tor network. And, finding that, that line that we shouldn't cross is . . . difficult, but I would say most people agree. There are certainly some people that think we should be 100% transparent, but . . . we've, as a group we've generally decided that

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

it's better to be slightly closed and reap some of the benefit from that, rather than be completely open and not be able to protect the Tor network as much.

Tor core developer

The notion of hierarchy is an odd one in Tor—as more developers joined the project, it became neither a leaderless collective nor a rigid hierarchy, but something more complex. Instead, its community members considered themselves a *do-ocracy*, with new developers generally taking full control of their own small projects or particular features of the Tor technology and contributing feedback, advice, and criticism for everyone else. Major decisions—such as whether to incorporate new features—generally involved the coordination of loose consensus, but much of this was set at the strategic level, driven by funding or new projects explicitly committed to particular aims, with any remaining discussions among the team left to matters of implementation. The idea of decentralization was still at the heart of this approach, as it minimized concentrations of power and influence and distributed key responsibilities among separate groups. At least in principle, this approach aimed to find clusters of power within the core team and use community design solutions to unravel them.

Yeah, well I think one of the things that's quite good about Tor, especially these days, is that we don't have kind of a really strong personality cult or something like that, where, you know, I think that Wikileaks partly suffers from that. I think, you know, any one person could have an issue or whatever, but it doesn't necessarily undermine the whole rganization . . . So you're more, I think it's more fragile [when power become concentrated], because it's really much more exposed to the mistakes of one person, let's say. I mean, Wikileaks might also be an example. But I think in Tor, it's not that there's no hierarchy, but there's a general feeling, I mean, we talk about a "do-ocracy" in Tor [*laughs*] which is, I don't think originates from Tor, I'm not sure where it comes from, but basically, like, you know, if you want something to happen, you just do it. And, and you don't have to ask permission for things, to do things, and generally speaking, people will respect you for the effort of trying to do something and, um . . . you know, and if someone does something really bad then the other people will try to fix it. It's like, there's not really a single point of failure.

Tor core developer

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

As these by-design structures hit the real world, the Tor Project quickly found that they didn't just work out of the box. Decentralizing human social structures was not always easy in practice. Many of Tor's users depended upon it in potentially life-or-death situations, and so its design processes required stability and careful judgement before radical shifts in design were made, so as not to endanger these users. A rigidly decentralized structure could make Tor vulnerable to a hostile takeover, or to well-meaning new community members banding together to push through a change that inadvertently put Tor's high-risk users in danger. As a result, in practice, a few key people within the organization retained an ultimate veto over Tor's technical direction.

> Within the Tor Project it's not easy to do any takeovers, because it's the main core developers. And I don't see why Nick Mathewson would have a change of opinion in how he thinks about Tor. Or Roger. Ultimately, I mean Roger's very accepting and very, kind of, trying to stay out of decisions now. And, kind of, secretly, I think, if there was something happening in that respect that would endanger, kind of, how everything is working technically, uh, they wouldn't accept that. So, I don't think there's a threat there or even a possibility of manipulation or anything.
>
> Tor core developer

This period saw not only the maturing of Tor's social structures, but also sweeping advancements in the technology itself. This includes, most notably, the creation of the Tor Browser—now the way that most people interact with Tor. In May of 2004, still the very early days of the network, Steven Murdoch, then a postgrad at the University of Cambridge, was invited to present a paper at the Information Hiding Workshop in Toronto. That year, the conference was being held in the same city as what is now called the Workshop on Privacy Enhancing Technologies (formerly the Workshop in Design Issues in Anonymity and Unobservability, the very conference at which Syverson and Dingledine had met four years earlier). Hoping to make the most of the long flight to Canada, Murdoch signed up for the second conference and sat through the talks, rubbing shoulders with a delegation of Tor's core crew—Dingledine, Mathewson, and a researcher named Peter Palfrader—as well as other anonymity researchers including Ian Goldberg

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

and Len Sassaman. After speaking with the Tor team, Murdoch agreed to set up a Tor node at the University of Cambridge's Computer Laboratory, where he was a researcher. Along with George Danezis, a long-time cypherpunk and also a graduate student at Cambridge, Murdoch would begin contributing to the Tor Project while also continuing his own research on attacks on anonymity systems. After writing a PhD thesis on Tor, Murdoch went to work at the OpenNet Initiative—a project tackling web censorship. With some funding from Tor (and later from academic grants), he then set to work on creating the Tor Browser.

In the mid-2000s, although Tor had been slowly growing its user base, usability was still a real issue. At the time, if you wanted to use Tor, you would have had to install and configure several different bits of software that together would package your traffic up, bundle an encrypted "onion," and then force your browser to route the traffic leaving it through the Tor network. For most of the everyday users that Tor aimed to attract, this was far too onerous. Even for the technically skilled, it was a real pain—having many separate "moving parts" increased the likelihood that you would configure something incorrectly or simply forget to activate a vital component. Vulnerabilities and bugs were being discovered and patched all the time, and keeping multiple bits of software configured and up to date was no simple task. This would limit the Tor network's users to privacy enthusiasts and technologists who saw it as a fun hobby and those motivated enough to get past these hurdles in usability. But this wasn't good enough for Tor's core privacy model. Most of those motivated enough by privacy to use a slow or cumbersome system would be those looking to break the law (whether for morally justifiable reasons or not), and thus suspicious to authorities, who could be pretty certain that someone was up to no good if they were using Tor. Restricting the user base in this way would greatly limit the size of the "crowd," and hence the anonymity protections which Tor could realistically provide.

The idea of usability has deep roots in the technical design of Tor, and widespread ease-of-use by the general public was a long-term goal, especially as successive funders complained about the clunkiness of its interfaces, the difficulties their desired users faced in operating it, and its slow network

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

speeds. In general, usability was presented as mostly a flat concept throughout this period of Tor's life, embodied by easily measured network speed and generic ideas of ease-of-use. But usability, as the developers would in later years accept, is not an obvious or neutral concept—there are many ways to make a technology more usable for different people, and to adapt design to different groups of users. This was tricky for Tor, which at this stage was still attempting to capture a vast, amorphous, and diverse set of users around the world. Thus, in general, improving usability required making the experience of using Tor feel as much as possible like using the regular internet—which meant a browser, and preferably one as recognizable as possible.

Rather than build something from scratch, Murdoch settled on an already existing browser as a base—the popular Firefox browser. Firefox was widely beloved, developed as it was by the Mozilla open-source project. To work properly with a browser, Tor required a lot of additional integration—most browsers had a range of security vulnerabilities and reporting functions which trivially de-anonymized their users and seriously undermined Tor's attempts to protect them. A plug-in for Tor in Firefox, called TorButton, had already been developed and fixed many of these issues. At the time, Tor itself didn't have a user interface; that came from Vidalia, a separate program again. Further questions emerged, questions that, again, seemed trivial but presented a number of security ramifications. For example, how could the various software libraries that all these things relied on be zipped up for users? Murdoch packaged up all the components of Tor in the Tor Browser Bundle and did the complex implementation work of distilling them into a single download that would work for users right away.[20]

In 2008, Murdoch released the Tor Browser Bundle, bringing Tor farther out of the bedrooms of computer enthusiasts and crypto-libertarians and into a much wider world of users. This was an important change in the *experience* of using Tor. It took Tor from a collection of esoteric programs and tools that modified how your computer processed its internet traffic, and turned it into a portal—a window that could let you see into a new space with its own characteristics. It made Tor look a lot more like the regular internet, and hid from the user the bits of tech whirring behind the scenes.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The integrated browser was crucial in forming the idea of Tor as a space of its own, rather than a set of technologies—a space separate from the regular internet, which could take on a more mysterious, darker character.

Further changes in the technology continued to reshape the experience of using Tor while leaving the basic paradigms and design of the network largely unchanged. Some of these changes became wider standards within the industry—for example, Erinn Clark led efforts to develop *reproducible builds*, a way of making sure that when you downloaded Tor, you could check that it hadn't been secretly altered or compromised in the process of turning the programming code written by its developers into lower-level instructions that could be read by your computer.

This also included developments in the relay network. At this point, if you were operating a Tor relay, it simply sat running in a command line, giving little feedback as to how it was performing or what it was actually doing. Though you were still contributing, it lacked the feel of a high-tech hacker project. And along with a commitment to the intellectual side of technology, the hacker underground has an equal if not greater attachment to the aesthetics of hacking—cool readouts, ASCII-art displays, and so-called *blinkenlights*, or arrays of flashing LEDs. Damian Johnson, a volunteer in the wider community, developed the Arm (later renamed Nyx) tool in 2009 to create what was effectively a visual display or monitor for Tor relays that ran in the command line. This was also a usability development, but in the opposite way as was the creation of the Tor browser—Arm foregrounded the technical work being done behind the scenes rather than hiding it, and it made the experience more technical and "hackery." This might seem simple or trivial, but it was in fact an important change to the relay network. It changed the core experience of running a relay, emphasizing the "gardening" aspect of contributing and making the act of tending one feel more real. Rather than an invisible thing running in the background, a relay was now something you could see on a screen, that was giving you feedback—beeping away like something from a hacker film.

As Tor set down roots, so did its cultures. Dingledine and Mathewson were still the ones with the keys to the kingdom—specifically, the cryptographic keys that would allow them to approve changes to Tor's

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

codebase—but the board of directors ran Tor as a nonprofit. In theory, they were tasked with setting its strategic direction, but in practice, the nonprofit culture was very separate from the technical work, which was largely driven by grants and practicalities. Balancing all this, and managing a very diverse community centered around three very different worlds—the more well-established engineer and maintainer worlds, and the embryonic NGO ambitions—took a great deal of delicate work.

Thus, over this "middle period" of Tor, there was a real advantage to keeping the core values of the organization a bit abstract. Tor was a technology project first and foremost—a container in which anyone could place their own personal politics, and come together with support, new tech, or funding for the infrastructure. The maintainers ran Tor as a service while the engineers slowly weaved Tor through the technologies of the internet. But this strategic ambiguity began to crumble in the face of a new set of challenges. The engineers had built Tor to snap together with other technologies—some of which unlocked radical new capabilities—and the growing roots of the infrastructure started to draw in communities that wanted to use Tor for their own purposes. Possibly inevitably, innovation in the criminalized parts of the hacker scene led to a new era of Tor. The Dark Web was coming.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

7 THE DARK NET RISES

Tor continued to mature and grow over the late 2000s and early 2010s, and so too did its user base. From an initial community of cypherpunks, members of the hacker scene, and digital freedom enthusiasts, the Tor user community slowly expanded to include a range of other, more diverse users, often with far less technical know-how. Between 2004 and 2009, due to progressive improvements in usability and speed coupled with more visibility through Tor's burgeoning partnerships with global civil society, the Tor network skyrocketed from thousands of users per day to hundreds of thousands.[1] With them, these users brought a range of new problems, many of which the Tor Project is still dealing with today. Although Tor's vision of reaching the general public was beginning to be truly realized, it was not always necessarily in the ways they had expected or hoped. A sizeable number of these new users were drawn not to Tor, but to its emerging shadow persona—the *Dark Web*.

The Dark Web can refer to a lot of different things, depending on whom you ask. Although it is a wildly misleading term, it is the name by which the vast majority of people know Tor—in fact, I agonized over whether to include the phrase in the title of this book, but eventually accepted that if I didn't, then very few prospective readers would have any idea what the book was even about. But even mentioning the term within the Tor community can cause controversy—in fact, when I used the term during an interview with one Tor developer, they sighed, reached under the table, got a laptop out of their bag, and then proceeded to give me a short PowerPoint presentation they had prepared earlier on why it doesn't exist.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Many academics and security professionals use the term *Dark Web* generally to describe web services hosted on the Tor network. These *hidden services* (now called *onion services*) use a so-called onion address to allow users to connect anonymously and also allow the website itself to hide its location and identity from the users, making them very difficult to shut down or censor. Most sites hosted on the Tor network are "legitimate" services seeking to resist censorship, such as blogs, wikis, and newspapers; a relatively small number function as marketplaces for illegal goods, host discussion forums for criminalized communities, or provide the technology for sites whose content is so controversial or objectionable that most hosting providers wouldn't knowingly provide them space to host themselves.[2]

This is often depicted using a much-derided diagram of the internet as an iceberg, with the "surface web" of easily accessed sites indexed by search engines as the visible tip above the water, and a vast aquatic bulk labeled the "deep web" below the surface. The latter includes all websites not indexed by search engines, or which require passwords to access (such as your Facebook account and Google Photos account, university libraries, corporate systems, and password-protected forums).[3] Under this vast bulk, at the bottom of the graphic, is the so-called *Dark Web* of sites only accessible using anonymizer tools like Tor, or alternatives such as the I2P peer-to-peer hosting service.

This graphic is, fortunately for internet users everywhere, nonsense. Claiming that all data stored in servers accessible via the web are part of a shadowy bulk of unindexed sites is misleading—the equivalent of saying that books indexed in your local library sit on top of a vast hidden "deep library" of books that live in people's living rooms, or arguing that all the ketchup that isn't stored in supermarkets exists in a shadowy "deep kitchen." It's technically true but tells us nothing about the phenomenon we're interested in.[4] What it does do is visually distort the size of the *Dark Web* by linking it to the disproportionately huge "deep web" in the iceberg diagram (often through the cringeworthy phrase "the deep dark web").

This gives the misleading impression that the parts of the internet that are indexed by corporations don't have abuse issues and can be easily patrolled by digital cops, and that the real crime problem is a vast sea of evil sites lying under the surface that the police can't touch. In reality, the vast

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

majority of online crime occurs on the regular internet, through abuse of social media sites, chat channels, or forums that can be accessed through a normal web browser or mobile phone app.[5] The hidden services on Tor, far from a huge, unknowable bulk hidden under the surface, are a tiny collection of mostly niche illegal markets and forums that spend a lot of their time knocking one another offline; a similarly sized group of wikis, social sites, and blogs; and legitimate services like Facebook (which now runs its own onion service), newspaper story submission portals, tip lines, and messaging programs like Ricochet.[6] Tor is often the last resort for sites who face serious public outrage—like neo-Nazi forums or sites devoted to transphobic harassment—and end up setting up far smaller and less accessible onion sites when their hosting providers drop them after a public boycott.

For quite a long time, the Tor Project avoided addressing the Dark Web much at all. On the face of it, looking back on a decade of media coverage of cryptomarkets, this might seem absurd. But to the Tor Project, the Dark Web really did seem to be something largely made up by the media. The Tor network wasn't some parasite attached to the "real internet"—it *was* the internet, one of myriad smaller networks and services linked to the backbone of global digital communications, each of which had its own topology, rules, and problems with abuse. If anything, Tor was a lot more like the internet that early pioneers—idealistic hackers, engineers, and hobbyists—*thought* they were building in the 1990s and less like the hyper-surveilled, overmonetized world of the social media platforms—the real parasites of the utopian internet, and the source of far more (and far worse) abuse.

Using the browsing functions of Tor for nefarious purposes—to download illegal material, organize criminalized communities, or visit illicit websites anonymously—represents a problem for law enforcement, but not an insurmountable one. Police have historically been uninterested in the sea of people committing minor crimes on web services, preferring for platforms themselves to monitor this type of activity. Instead, police are generally concerned with cutting off the sources of online crime—websites and services that host illegal material. This is partly a result of how policing is organized in most countries: local cops lack the technical skills or international connections to deal with cybercrime, so it is generally handled by centralized

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

agencies like the FBI that are more equipped and accustomed to taking down serious organized crime groups.[7] Their technique of choice has long been disruption—identify and arrest the suspects (if they're in your jurisdiction), take down the servers (if they're hosted in your jurisdiction) and seize the assets.[8] Tor doesn't help you much here if you're committing a crime—it's easier just to move house to a friendly jurisdiction and host your site in Russia. But the police *can* get ISPs in their jurisdictions to block the public there from accessing a certain website—making actually taking it down and arresting the host someone else's problem.

However, a more radical function of the Tor network would grow to predominate discussions of online abuse, and would come to present law enforcement with what it would begin to see as a real challenge to its authority over the internet. Since the earliest days of Tor, the network was designed not only to carry browsing traffic, but also to host websites and services (recall Dingledine's initial visions of a decentralized file-hosting network for Free Haven). As early as 2003, the project released a design for what was then called *hidden services*. By linking two onion circuits together so that they met somewhere in the Tor network (called a *rendezvous point*), you could turn Tor upside down—as well as browsing the internet, you could now use Tor to host sites anonymously. By setting up an *onion address* that led you through the network, you could leave a marker for people to visit your site without leaving a trail back to you.

If these rendezvous points sound like a Cold War *treff* between East German spies, then the technical reality isn't far off—a game of note-passing in the foggy, romantic city of the relay network. The creator of a hidden service sets up their website much like any other—by hosting it on a normal web server somewhere on the regular internet. Tor's software then creates a document for them that functions something like a coded map, a list of six relays in the Tor network that can serve as *introduction points* for users to access their service.[9] This map (along with those for other hidden services) is stored in a directory that is distributed throughout the relay network, living in chunks and copies so that no single relay contains or controls the full list of hidden services. When brought together, these chunks create something like an atlas of the hidden services in the Tor network. Only relays that have

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

shown a decent record of stable, non-suspicious behavior can opt in to host part of this hidden directory service.[10] At regular intervals, the hidden service will post its map fragment onto six relays in the network, allowing users of the network to scan through and find the introduction points for the services they want to access. A prospective user then sends a message to their service's introduction point, asking it to pass on a request to the owner to meet them somewhere else in the Tor network—setting up another relay as a rendezvous point. They each then build a standard three-hop anonymous Tor circuit to the rendezvous point—the equivalent of an innocuous cafe in the suburbs of our Cold War city—which then passes messages between the hidden service and the user, allowing the user to view content, send signals, and generally use what feels like a normal web service.

So rather than the browsing function of Tor, which mimics a spy taking a circuitous route through the city to get to their destination, changing their path each time, hidden services operate more like a spy trying to set up a meeting with an informant, all the while hiding the location from each of their employers. This game of cat-and-mouse is far less complicated to set up than it seems—the network does much of this work for its users automatically. For the user, all you need to do is launch the Tor Browser, paste in your service's *onion address* (a long string of characters ending in .onion rather than .com) to the address bar, and you're taken to where you want to go. These addresses themselves have very clever properties—they act as their own kind of cryptographic signing code, allowing you to verify their identity.

In 2004, the first hidden services were deployed on the network—mostly fairly innocuous blogs and online file dumps of vaguely libertarian books like *The Anarchist Cookbook*. The development of hidden services was a natural progression for Tor, shifting its focus from its anonymity features to increasingly prioritize censorship circumvention. This shift in focus fit well with the alliances it was making over the 2000s with the organs of US soft power, as authoritarian nations ramped up their efforts at online censorship and more internet users wanted to publish their own content in addition to browsing the offerings of Western media. But from these small beginnings, this capability would eventually catapult Tor into the public eye and pose an existential threat to the network.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The increasing numbers of hidden services springing up over the mid-2000s did lead to some early experimentation by some users for illegal businesses, but these services initially enjoyed only fairly limited commercial success. First, true anonymity is a terrible model for a criminal enterprise, which generally must build and maintain trust and reputation to avoid becoming riddled with scams. Second, lucrative illegal markets generally need a way to send and receive cash. Although there were some existing ways to do this anonymously in the mid-2000s—trading in digital assets like Amazon vouchers and Counter-Strike weapon skins, or in currency systems like Liberty Reserve and Western Union—there were few foolproof ways to get money to someone without a bank transfer. Although the Tor network might hide your digital identity, in practice, *payment* was fairly easy for banks and police to track. The global rich had complex networks of shell companies and offshore registrations to hide the flows of their money—and while organized crime groups did too, their customers and lower-level dealers generally didn't.

The rise of another decentralized network helped fill this gap. Some of the cypherpunks had long sought a way to transfer money without the government getting its hands on it—for tax, censorship, or surveillance purposes. Much like anonymization networks, proposals for digital cash had existed for a long time, going back to papers by David Chaum, the inventor of Mixnet anonymity networks, as early as the 1980s. Bitcoin was an implementation of an idea that Chaum had proposed in 1982 as a form of digital cash that relied on a distributed system of accounting ledgers that would all check in with one another regularly and make coordinated, cryptographically verified updates to a shared list of transactions.[11] These transactions would be carried out in a shared currency that would act as a store of value. This idea—called *cryptocurrency*—had developed in fits and starts across the 1990s much like onion routing did, with small test networks, mini-projects, and trial runs within the cypherpunk community. As we can see, time and again, these very similar systems and designs have mimicked and matured alongside each another for decades. In 2009, a mysterious developer using the name Satoshi Nakamoto would launch the Bitcoin design, a type of cryptocurrency that

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

forced the infrastructure network to run complex calculations (called *mining*) as it ticked through each new set of transactions, with the ones that did so fast enough being awarded some of the digital cash used by the network.[12] This generated scarcity in the novel electronic currency, which, when combined with hype, meant value.

What Bitcoin developed into looks much like a version of Tor but designed for anonymous money rather than anonymous web browsing: a decentralized network of servers that together (in theory) short-circuit the ability of states and corporations to control and censor global flows of information.[13] Much like Tor, its value is proportional to the number of people using it; with Bitcoin, however, rather than accruing anonymity, early investors accrue more value. And much like Tor, it has been prone to centralization, with the distributed network of miners coalescing around a few very large mining operations, and much of the network's cash value being concentrated in the hands of a very small number of investors.[14] However, while for Tor a great deal of effort goes into *reversing* this centralization, the financial incentives for Bitcoin users and miners point in the other direction.

Thus, it's no surprise that (outside a few dissenting voices and attempts to fork the technology), there has been a general drive for the network to prioritize financial gains for speculators, early adopters, and big investment funds, rather than evolve as a technology for the liberation of public finance. Bitcoin took some time to really take off—in its early days it too was mostly confined to the libertarian cypherpunk crowd and their descendants in the underground hacker scene. But Wikileaks entered the story again here, playing a key role in driving public attention to the nascent Bitcoin network.

In 2009, US Army intelligence analyst Chelsea Manning was deployed with her unit in Iraq as part of the US occupation. There, she had access to vast reams of operational data—and, as she trawled through intelligence reports, grew increasingly disgusted with her own government and military. The following year, in 2010, she would go on to contact Wikileaks founder Julian Assange over the Tor network (having first tried the *Washington Post* and the *New York Times*, with no success), eventually leaking nearly 750,000 military and diplomatic documents. The most famous of these,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

which became one of the defining images of the war in Iraq, was a video titled *Collateral Murder*, in which the crew of an Apache helicopter were recorded firing on and killing civilians on the ground.[15]

This enormous leak of military and diplomatic data catapulted Wikileaks and Manning to global fame, while drawing public attention to shocking abuses by the US military. The backlash was severe—after being tipped off to law enforcement by undercover informant and former hacker Adrian Lamo, Manning, who became a hero to the digital freedom movement, would be sentenced to 35 years in prison (after being acquitted of aiding the enemy), though she would serve just over six before having her sentence commuted by then-President Obama. Wikileaks also faced serious sanctions, with several major banks blocking donations. The cypherpunks were united in condemnation of what they saw as major financial institutions uniting to advance the interests of the United States. This enormous mobilization of structural power against Wikileaks drove attention in the cypherpunk community to the young Bitcoin network as a possible way to avoid these kinds of sanctions, stimulating research efforts around other cryptocurrencies. In 2011, having initially held off for fear of swamping the fledgling Bitcoin network, Wikileaks began accepting donations of Bitcoin.[16]

As Bitcoin began to spread among the techno-libertarian internet underground, new services began to emerge, combining the anonymity properties of Tor with the censorship-free financial networks created by Bitcoin. But Bitcoin had a problem—although it was a *cryptocurrency*, the cryptography was used to verify transactions rather than hide them. It operated on a publicly distributed ledger, meaning that all transactions were publicly recorded. Bitcoin does nothing to hide your identity, so if you are a government or private security company, you can trace wallets and transactions on the chain. The government can also block your commerce website and track who goes there, thus linking a wallet address and what it does to an individual user. At the same time, Tor has a mirror problem—you can't really use it for commerce, as the banks can trace and block the transaction at their end, thus allowing you to link financial activity (and hence web activity) to a real person. But by combining Bitcoin and Tor, you can make it very hard to show who owns a particular wallet, and can carry out commerce "in the dark."

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Ross Ulbricht, a young entrepreneur and enthusiastic libertarian, had spent the mid-2000s operating a series of doomed commercial ventures. Operating under the name *Dread Pirate Roberts*, Ulbricht set up a Tor hidden service called Silk Road in early 2011, cobbling together bits of libertarian philosophy and half-understood code. After advertising the site on the Bitcoin forums and selling small amounts of psylocibin mushrooms to interested buyers, business began to pick up, and over the next year Ulbricht would rework the site, hiring administrators, automating key functions, and turning it into the first successful cryptomarket.[17] Silk Road operated much like other e-commerce sites of the time—the press called it an "eBay for drugs," as vendors would set up individual profiles and sell their inventories to customers, with Ulbricht taking a cut (though much of its sales were effectively business-to-business).[18]

In addition to solving the problem of traceability for its users' money and internet traffic, it also took a number of technical design innovations from the emerging e-commerce world. Prior online sites for illegal products had tended to quickly become "lemon markets" as the incentives to rip people off in truly anonymous environments are greater than the incentives to trade fairly. The Silk Road implemented a reputation system somewhat like eBay's—traders would accrue a reputation based on successful transactions, and would accumulate reviews of their products and customer service. Attached to this was an escrow system—the marketplace itself would hold the buyer's money and release it to the vendor when the product arrived. This incentivized small-scale, low-risk trading for new entrants to the market, which would then build up into established networks of business relationships over time.[19]

Between these two innovations—providing built-in operational and financial security—Ulbricht had created a business and technical model that would prove a runaway success. The early adopters and first users of Silk Road were mostly quite like the cypherpunks—people who combined a strong sympathy for libertarian values with technological utopianism and an enthusiasm for small-scale drug use.[20] But Silk Road didn't stay secret for long. As academics and journalists started to visit, and word began to spread online, the user base expanded far beyond techno-libertarians and Bitcoin enthusiasts. Following a profile in Gawker in 2011, new users and millions

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

of dollars flooded into Silk Road.[21] As Ulbricht's profits ballooned and the site expanded, his actions became increasingly paranoid and bizarre—the platform riven with infighting and backstabbing between the administrators he had hired to help him.[22]

This all came to a head in 2013—only two years after the launch of Silk Road. With the growing media attention and popularization of illicit use cases, law enforcement—particularly the FBI—was anxious to assert its ability to police these novel "dark" online spaces. Although Tor was successfully protecting his metadata from law enforcement surveillance, Ulbricht had made a number of mistakes. In particular, he had posted a number of times on the Bitcoin forums (and elsewhere online) using his Dread Pirate Roberts pseudonym, but had left his personal email as a contact. This led law enforcement straight to him—and to his arrest. With Ulbricht's arrest, and the huge wave of international news coverage of what he had been doing, the so-called Dark Web really broke onto the world stage.[23]

Far from breaking the cryptomarket economy, Ulbricht's' arrest and the shutting down of Silk Road was like throwing a can of gasoline onto a fire. The huge publicity generated by the bust led to millions more people around the world finding out about the existence of cryptomarkets and the shadowy Dark Web. Before long, a successor service—Silk Road 2.0—was set up by former administrators of the original site, and, the original monopoly broken, a scattering of competitor markets began to emerge.[24] Tor itself benefited from this surge in interest—search traffic for the Tor Browser doubled in the aftermath of the raids.

Law enforcement would hit back hard. In November 2014, the FBI and the European Union's Europol launched Operation Onymous, targeting a number of cryptomarkets that had sprung up to replace Silk Road, including Silk Road 2.0. Although most of the hidden service sites they took down weren't cryptomarkets, they did manage to take out several of the major markets trading at the time, seizing their customer databases and funds. They claimed to have taken down over 400 sites; in fact, many of these were clones or alternate links for the same few services, and the actual number was likely in the low dozens.[25]

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The operation was greeted with some dismay by the wider Tor community—although few were happy about the presence of cryptomarkets on the network, that law enforcement was able to pull off such an operation strongly implied either wholesale government compromise of the network or a serious unknown vulnerability.[26] In fact, the reality is more prosaic. As shown since by Sarah Jamie Lewis' OnionScan mapping project, hidden services are easy to misconfigure, and large proportions of the ecosystem were making rookie mistakes that allowed them to be discovered. [27] There were also a range of other ways to find and arrest people using Tor, including exploiting bugs in higher-level parts of the Tor program like the browser, tracing Bitcoin transactions, tricking people with covert informants and undercover agents, or operational security failures with other services used by people accessing the Dark Web, all of which could, with enough resources expended by law enforcement, compromise their identity.

At the beginning, the cryptomarkets drew heavily from cypherpunk culture—reflexively anti-government, techno-libertarian, and enamored with the idea of truly free markets that could exist outside the state entirely, they were underpinned by technology rather than banks and law enforcement. But as police raids hit the marketplaces and people began going to jail, repeated crackdowns would change the culture of these illicit spaces.[28] For the libertarian users, the negative associations and police pressure (along with the rapid rise of a more mainstream community around cryptocurrency buoyed by hyper-charged wealth) seemed to genuinely dissuade them, but a much larger community was growing, interested less in techno-utopianism and more in the practical benefits of onion services. The raids and takedowns united this group together—against the cops.[29] The communities that grew here developed their own, more entrepreneurial culture and a privacy world focused around anonymity as a social experience in its own right.[30] They argued, not without justification, that cryptomarkets allowed them to mitigate much of the harm associated with the drug trade—improving the quality and price of drugs, allowing for better testing and safer buying, massively reducing the intercommunity violence associated with the drugs market, and protecting users from the harms of over-policing.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Left alone in fairly stable communities, these buyers and sellers could share safety practices, both for evading law enforcement, and for reducing the harms of the drugs they were consuming.[31] Far from lawless spaces, they developed their own moral codes—when the opioid crisis was sweeping across the United States, many cryptomarkets explicitly banned the sale of fentanyl on their sites, arguing that they didn't want to see their users dying on the streets. While some were purchasing kilos of hash, others were using these markets to evade the state in different ways, to buy prescription drugs that were banned or unaffordable in their countries, to get safe abortion services, or to buy hormones for gender transition.

Jumping to the present day, cryptomarkets still exist but look quite different from their early incarnations.[32] They mostly act as a bootstrap for building a reputation and making connections, with people buying small amounts, developing relationships with dealers, and then transferring to encrypted messaging services. The markets themselves don't tend to last long—they spend much of their time knocking one another offline, and are still subject to periodic takedowns by law enforcement. And the escrow system, while being very effective at disincentivizing fraud among the people using the market, created a massive opportunity for the sites themselves to scam their communities—as they grew, the amount of money the sites held in escrow did as well, as did the likelihood of arrest. After a certain point for any successful cryptomarket, the rational move always becomes to walk away with everyone's cash—so you have to be pretty committed to the community to stay in it for long.[33]

Although the Dark Web has long been associated with drug markets, its technical sheen has led many to assume that it is a haven for cybercrime groups too. But this too is a misconception. Cybercrime groups have evolved significantly since the anarchic days of the early underground scene. In the late 1980s and early 1990s, the people testing and building new tech, or trying to disrupt and subvert systems, were often the same people being labeled as criminals or targeted by the police. As the tech boom of the late 1990s took off, much clearer routes emerged into professional security jobs, for example by working for the government or the bustling start-up entrepreneur

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

economy. This only developed further in the late 2000s, as hackers began to increasingly link up with activists and social movements.[34]

Nestling around their own forums and instant messaging channels, the cybercrime and hacking scenes continued to separate over the early 2010s. The economy of cybercrime had changed. For decades, cybercrime communities had been a tool-based market—with a small group of technically proficient hackers developing new tools for breaking systems and selling or trading them to a much larger community of *script kiddies*—low-skilled hackers who would buy the tools and use them, eventually learning technical skills themselves. These cybercrime communities were committed to the *hacker ethos*, valuing technical mastery, experimentation, and expertise. But like many economies, the cybercrime underground was beginning to industrialize, shifting to a service model. Rather than build and sell tools, it became far more profitable to sell access to them as a service, turning the work of cybercrime from innovative hacking into customer service work and systems administration. In fact, most of the people hanging around on these forums, and even those running quite lucrative cybercrime businesses, lacked much in the way of technical skill or sophistication at all.[35] The values began to shift—away from the hacker ethic and towards a rise-and-grind, entrepreneurial, small-business mentality. Most (but not all) genuinely proficient hackers ended up moving pretty quickly into the spy agencies, security firms, or occasionally into more serious organized crime groups.[36]

The cybercrime underground initially showed some interest in hidden services, but for most, the Dark Web was simply not as useful as sites on the regular internet. This ecosystem of hackers and scammers were organized around online communities and small businesses—and their customers weren't particularly technical, generally prizing user experience over security. In fact, several hacker forums began to explicitly block users connecting from Tor in order to avoid spam comments, people evading IP bans, and researchers and police from scraping them. Tor became a common recommendation for keeping yourself safe from law enforcement, but there was little connection with the cybercrime communities themselves, whose interests were moving from technical exploitation to leaks, scams, and frauds, often

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

through taking over people's social media accounts. Instead of becoming a cultural home for the cybercrime underground, cryptomarkets and Dark Web forums became a place for trading leaked datasets and for smaller, invite-only communities. If you had some stolen credit cards or compromised accounts and didn't have decent connections, you could find your way to a Dark Web site and have a chance of finding a buyer. These sites became a social network for low-level crime that used Tor to build in basic security practices by default.

There were two major exceptions to this—areas where the cybercrime underground found a use for Tor beyond simply hiding their web browsing like everyone else, or hosting underground data exchanges and forums. The first was the explosion of botnets in the early 2010s. A botnet is a form of cybercrime infrastructure—a virus spreads across the internet, infecting vulnerable computers and taking them under control, building into a distributed network not unlike Tor. This network can be controlled from a centralized command-and-control server owned by the botnet *herder*, and used for a variety of purposes, from knocking computers offline to mining cryptocurrency. Tor was seen as useful for hiding this command server, allowing the network to live on even if a few bots got taken down.[37]

The second was ransomware, a type of virus that lodges on the target's computer and spreads through its network, slowly encrypting each of its files and databases one by one until the whole network is compromised, at which point the owner receives a request for money. This kind of attack proved so lucrative that ransomware gangs began to spin up their own human resource departments and customer service staff to manage the flow of victims and money. However, gangs were increasingly finding that their victims were struggling to pay their ransoms anonymously, and so used a series of technologies, including Tor2Web (a service that allows you to access hidden services from a normal browser) and Bitcoin to receive ransom payments.

In the last ten years, both botnets and ransomware have largely evolved beyond the need for Tor. The cybercrime underground has developed a sprawling economy of dodgy *bulletproof hosting* services, or servers located in countries and providers that don't respond to law enforcement requests

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

and are hard to take down, and so provide many of the same functions as the Tor network but with much faster speed.

The spy agencies of Western governments had a rather different view of Tor. While certainly on board with the soft power aspects of the network and its utility as a go-to anonymous communication system for human intelligence sources in the field, their own threat models were changing in the mid-2010s. As the War on Terror continued, it was evolving—no longer were the spy agencies trying only to deal with military-style hierarchical terrorist organizations operating in cells, but also with a far more diffuse kind of radicalization. Waves of attacks in London, Boston, Paris, and other major cities were being carried out by young men with no formal connection to hierarchical terror groups, but who had been radicalized online. This intensified an already growing desire for agencies like the UK's Government Communications Headquarters (GCHQ) to be able to develop bulk traffic intercepts—the capability to sift through huge reams of data with machine learning technologies developed by their researchers to find clues and signals. Although in fact it was mostly not used by terrorists, growing use of Tor could make this kind of mass surveillance far more expensive, or break it entirely.[38]

While some of this was a matter of strategic state power, a genuine disgust had begun to emerge in some corners of GCHQ for the Tor network. Although the average member of technical staff (a *nation-state hacker*) was not politically dissimilar from the cryptographers and engineers in the Tor community, GCHQ had grown into a major civil service department. Not everyone working for them was a technical analyst, and plenty were more involved in project management, policy, and outreach to the corporate sector, defense, or law enforcement. Seeing online child abuse as predominately an internet matter, the UK government had tasked GCHQ with supporting law enforcement in tackling it, leading to a sizeable chunk of work.

Your idea of the causes and solutions of a problem depends largely on which agency you ask to deal with it. GCHQ is a signals intelligence agency, and so its ability to respond to threats is dependent on its surveillance picture of the internet—much like Tor's developers idea of *privacy as*

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

a structure, GCHQ sees crime as a problem of network structures and law enforcement's ability to observe and control them. For this, Tor does prove a real problem—especially as these child abuse communities were mostly not markets, instead trading material for free, so there was often no currency to trace. For many in the agency, especially around a small number of particularly upsetting cases, this went beyond a policy issue and became a personal one. Dealing with this material every day and seeing some of the most shocking forms of harm and abuse proliferating in the handful of small, closed abuse communities on onion services did little to endear them to the network. In fact, for some of the most egregious and harmful individuals, who were particularly adept at using technologies like Tor to hide from the state, GCHQ mobilized huge numbers of staff and resources to deanonymize them. While not calling for a ban on Tor, they redoubled efforts to compromise the network technically, and in this spirit, GCHQ and the UK's National Crime Agency formed the Joint Operations Cell in 2015.[39]

> The so-called "dark-net" is increasingly used by paedophiles to view sickening images. I want them to hear loud and clear: we are shining a light on the web's darkest corners; if you are thinking of offending, there will be nowhere for you to hide.
>
> David Cameron, then UK Prime Minister, 2015

As law enforcement sounded the alarm, journalists and politicians jumped on the chance to make Tor the focus of swirling public anxieties about the internet more generally. Despite the realities of online crime, reputation and image matter greatly for technical projects. Although Tor purported to be designed for just about *anyone*—the generic privacy-conscious web citizen—it in fact had indirectly cultivated particular user groups, either through informal community links, ideological and cultural common cause (as with the Chaos Computer Club and the hacker underground), or formal collaborations, as with the Electronic Frontier Foundation, which provided Tor a link to wider internet freedom activist communities. As the Dark Web grew, Tor began to develop a reputation in the media as the go-to place for online crime. This threatened to become a self-fulfilling prophecy, with media coverage itself advertising Tor as a criminal network.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

New communities on the cryptomarkets began fashioning their own identities and cultures around the Tor network, which proved irresistible for a generation of fiction writers and television producers. In the world of fiction, the *Dark Web*, Tor's alter ego, began to appear everywhere as a cipher for online evil—from William Gibson novels, to television shows like *Mr. Robot*, video games, and even rap songs. As the web became part of our everyday lives and lost its mystique, its Dark Web cousin provided a way to return to the 1990s image of the lawless internet. This media reporting spiraled out of control, with Tor quickly becoming eclipsed by its Dark Web alter ego in the public eye. Lurid (and often apocryphal) stories about hitman-for-hire services, gun smuggling, and horrendous crime abounded. Although few nations criminalized Tor, some attempted to block it entirely, using Tor's crime-ridden image to associate it with child sex abuse, drug trafficking, and terrorism rather than free speech and resistance to censorship.

There certainly are harms that proliferate on Tor (as there are on the rest of the internet). I would argue that it is more useful to assess what the general effects of a new technology like Tor are for a particular type of harm and how central the privacy properties of these technologies actually are. How, if at all, does a technology like Tor actually empower the person committing harm, are alternatives readily available, and how does the privacy provided by that technology relate to that harm as it exists in wider society? Child abuse communities do indeed use Tor to communicate and share images and videos of abuse—and this is morally abhorrent. But the problem of child abuse is enormous and largely not an issue of the relatively tiny numbers of people who use Tor. The vast majority of child abuse does not occur online—it happens within communities, often hidden not by the onion network, but by institutions and by patriarchal power. Of that which does occur online, very little actually relies on Tor—in fact, almost all social media companies have full-time teams working to take down the seas of abuse content posted on their platform (on the regular internet), whether in encrypted direct messages or simply out in the open on their site. Tor's function in this ecosystem is to provide a small amount of protection to a small number of "hardened" distributors, but these people are themselves not reliant on Tor; they can get much the same functionality from buying a

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

couple of VPNs and servers in countries without criminal justice cooperation arrangements. Wealth and power, the complicity of institutions, governments and communities that ignore the rights of children and disbelieve and disempower them—all of these provide far better privacy protections for child sex abusers than the Tor relay network ever could.

At this point, an observer familiar with Tor's history and values might ask: when it comes to instances of online harm, what makes Tor more responsible than the rest of the internet? Why should Tor bear responsibility for the bad things people use it for any more or less than the internet service providers, or the companies that make fiberoptic cables? If anyone can set up a website with a Russian hosting provider or buy a dodgy VPN to hide their traffic, what does Tor actually change? For a long time, this was a persuasive view within the Tor community—that misuse was an issue of administration and maintenance, rather than moral responsibility. But the public relations blows Tor was sustaining over reports of crime were not the only problems it faced—in fact, abuse of Tor was threatening the relay network and its administrators.

From a designer's perspective, the Tor network's rearrangement of the topology of online space and power works smoothly. Tor takes an internet in which power is concentrated at the internet service providers, breaks that power up, and spreads it around a decentralized network. But the power of law enforcement isn't dissipated quite so simply—instead it is merely refocused, coming to bear against the infrastructure itself and the people who make it work. For law enforcement to gather evidence on the internet, they rely on the infrastructure—the platforms and internet service providers and their logs of what people are up to. An attempt to visit an illegal website, for example, might cause the internet service provider to raise a flag to law enforcement, or a search of an abuser's property might yield a laptop with evidence of illegal activity, in which case the police would approach the ISP to ask for records of the IP addresses of those accessing the illicit service.

All of this assumes a basic feature of how the internet works—as far as the infrastructure is concerned, you are your IP address at a given point in time. If you use Tor, this IP address will belong to a Tor exit relay—the last hop taken out of the Tor network, owned and operated by a volunteer. This

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

poses serious problems for the volunteers who run the Tor relay network. Rather than the Tor network simply "separating your identity from your traffic," it instead might be more accurate to say that it pins your identity on a randomly selected exit relay operator. To the police, it can appear that the owners of these exit relays, which make hundreds or thousands of connections to websites each day, are themselves visiting vast numbers of illicit sites.

> Because the moment where, kind of, if there's a small police, law enforcement office somewhere and they get an IP address and they ask the ISP who was the customer who was using that IP address, and then they get a customer record, and then some small town policemen go and get some small town court to, say OK, and they come to your door, it's already too late. Like, you have to kind of sit back and allow them to, basically, take all your hardware, and then later argue that there's enough proof that you weren't related to the crime.
>
> Relay operator

Across the world, this law enforcement attention on the relay network ramped up significantly, with some relay operators facing dawn raids, equipment seizures, and lengthy court cases. Particularly in Germany and France, a wave of raids began to exert serious pressure on the network.[40] As one of my interviewees said:

> It is actually a terrifying experience. Um, I wouldn't wish that to my worst enemies . . . They wake you up, at five minutes to seven in the morning, after, with my sleep cycle, I'd had two hours of sleep that day . . . And then, uh, ding-dong, welcome . . . we have a . . . search warrant, yes, that's it. Um, and they're standing at your door, with four people, and once you open the door, there's a foot in the door . . . Even if . . . once you've had a police raid for child porn, that's, you can't burn your name more than that. Something always sticks.
>
> Tor relay operator

Despite these traumatic raids, the relay operators mostly managed to stay out of jail (except in the rare cases where someone would set up an exit relay and then use it as a cover for their own illegal activities). But in other countries with more explicitly authoritarian domestic policies, operators faced far more severe penalties. In 2017, a twenty-six-year-old Russian math teacher and relay operator named Dmitri Bogatov was arrested under

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

anti-terror laws for running an exit relay after someone had allegedly used his relay to post a message calling for violence at a protest. After spending months in prison, Bogatov was eventually acquitted of the charges.[41]

The negative publicity, dismissed by many in the Tor community as meaningless newspaper hysteria, was beginning to take a toll on relay operators, who were trying to explain to their family and friends why the hobby project or volunteer work they were spending their weekends on was appearing in the press as the new frontier of online evil:

> I have some people asking me "Hey, some weeks ago you told about Tor Browsers and something, what are you doing there? Are you buying drugs, are you buying guns?" And I told them, no—I was looking for some alternative, uh, news and I visit some websites, I don't want to leave any footprint. That's my reason I'm going there. And they all asked "Huh? I thought myself it's just for buying guns and abusing children!" and I said to them "No! it's just an Internet without Google and Facebook."
>
> Tor relay operator

Over the years, the people who run the Tor network have largely adapted to these problems. The relay operators, encouraged by the Tor Project and by necessity, began waging a public relations campaign of their own, speaking to internet service providers and police services about what Tor was and about its various benefits. Showcasing their commitment to the traditional hacker way of finding clever technical workarounds and loopholes, the relay community also came up with a range of schemes for evading law enforcement. The first, and most basic, workaround is simple: don't run an exit relay from your home internet connection. As obvious as it might seem, this was important because it meant that if you got raided, you just lost your relay, not your personal hard drive and computer equipment. Relay operators also started coming up with clever legal arrangements, registering themselves as charities or internet service providers, and taking advantage of *mere conduit* protections that apply to the infrastructure providers of the internet backbone.

> When I run an exit, I want it to be owned by a legal entity that's not me. And that's for the risk of it being, if someone uses that, when someone uses that

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> exit for something bad, and some police investigation happens, which unfortunately might happen, I want the chain of, I want it to go to the company that owns it, and then at least it'll mean that they'll ask a question before they bash my door down. . . . I want it to be obvious when a police investigation is happening that this is a proxy, and so incorporating it is essential for me—I'm not going to run it in my own name.
>
> Tor relay operator

To help further, the Tor Project set up a service called ExoneraTor to protect its relay operators. It would allow a relay operator facing legal troubles to prove that on the date in question, the IP address the police were interested in belonged to an exit relay in the Tor network, rather than their personal computer. These administrative hacks, along with others, often made the difference between a boot in the door followed by a court case, and a polite letter asking for subscriber data. For those who did go to court, the Electronic Frontier Foundation signed up to provide (in most cases) representation and advice to those in the United States, and assistance to operators in other countries.

At this stage, in the early 2010s, Tor's implication in cryptomarkets was met with bemusement by most of the community. It seemed to be the same problem that Tor had always faced—much like the internet, phones, and the telegraph before it, some of its users wanted to use it for crime. But society took a rather different view. At this point, Tor's two main cultural worlds had rather different views on the crime problems Tor was facing. For the maintainers, privacy was a service—and criminal misuse was a problem faced by more or less all service providers.

> Because the tool is something that helps you to do something. But uh, you know, what you will do, with this tool, is up to you. Crime happens not on the hard drive of the Bond movie producer, crime happens not on the Silk Road drug store, no. Crime happens inside people's mind . . . Neither Tor or other software authors, nor people who are running even exit nodes, no they're not responsible. They are not responsible for another people's thoughts and actions. They are not. Tor is just a tool.
>
> Tor relay operator

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Crime was therefore, to the people immersed in this culture, a matter of *administration*. Many of the relay operators were accustomed to this view, either working at internet service providers themselves, running small open-source projects, or working in IT jobs. Where people misused their systems, which they always did, it was rarely seen as a reflection of the morality of the service itself, but more as abuse on the internet that had to be managed. This led to some interesting clashes—for some of the operators, onion services are a service like any other. But many of the people I spoke to expressed frustration at what they saw as a secondary part of the Tor network that made the rest of it look bad. A number of relay operators explicitly said that they personally despised onion services—which they saw as largely used for crime—and wished that public attention would focus on the vast majority of Tor traffic, which was just used to browse the normal web privately.

> I'm not really a fan of onion services myself. I think it's nice from a technology point of view. It's nice if you can think about systems, and that's kind of the classical thinking that I was used to before all this public visibility. That kind of, the technical community accepts that it's currently all crap, and all shit happening on the Darknet. Because it's technically so neat . . . Just because you read a sci-fi when you were twelve, and in that sci-fi novel, the hero extracted all the data and fucked up all the big corporations that ruled the planet . . . I'm not sure that just because there are potential worlds where Hidden Services would save the planet, um, it's maybe not the world we live in.
>
> Core Tor contributor

> I think it's an absolute disaster . . . Tor's public perception has been really bad . . . if you look at it from the outside, it feels like some underground, dodgy, like, drugs trading thing. My really specific recommendation to them is to separate Hidden Services, because this whole, like "Dark Web" bullshit has come about from the fact that Tor enables Hidden Services, means that Tor gets lumped in with Silk Road. And that's not helpful, and I think the Tor Browser could really do with a rebrand . . . Tor Browser is about browsing without censorship.
>
> Relay operator

The engineer world, on the other hand, often saw crime as a red herring—an age-old response to social issues and other external causes that

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

happened to be appearing on Tor much as they would in any other system connected to a "real world" full of forces causing crime. If anything, Tor simply made these things *more* visible, surfacing the tip of an iceberg of real-world harms into internet spaces that could be accessed by the public and by law enforcement. Understanding privacy as a structure meant understanding crime and law enforcement as structures, too. For them, Tor was working as intended, forcing governments to stop looking for silver bullet technical solutions and pushing these problems back into the realm of democratic public policy.

> It's kind of a bit like MP3, where you say, OK, society might not be ready yet and we will kill a lot of stuff and, and . . . video killed the radio star! And it's like, technology comes first and then there's a struggle in society on how to restructure itself to be able to cope with that change. And I think a lot of the hacker ethos is about seeing what would be possible with technology. And, and seeing that there's all these forces that drag down the change, because they want to survive . . . All these structures are becoming more and more stale and static and, and, uh, the only way to change them would be to break them. And I like fluid systems. I like, this kind of structurelessness and, and chaos, and I think that's a value by itself, and . . . maybe that's the way to go, is to build these systems and then say, OK, maybe we will be fucked for thirty years because of these systems, and everything will go to shit, but afterwards we will rise again and a new society will evolve that is much better than the old one! I don't know.
>
> Tor core contributor

There were some more practical considerations backing up this view—a point made many times throughout the Crypto Wars. If someone is sitting on several kilograms of heroin, shutting down their onion site is unlikely to make a serious dent in their ability to find willing customers.

> If Tor were to go away tomorrow, the bad people would not really be inconvenienced very much . . . I think the only people who'll be significantly inconvenienced by the lack of Tor will be the, the relatively vulnerable people who aren't able to run their own network, and they'll be the people who don't want to break the law. So, I think, in that sense, Tor is, is overall positive. Um, regardless of how people are actually using it.
>
> Tor core developer

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

However, as time went on, the association with crime was beginning to cause serious problems for Tor, impacting its ability to raise funds and partner with other organizations, drawing huge amounts of law enforcement attention, and turning off some of the users who could benefit from it most. The negative attention also began to undermine Tor's security—as Tor became more and more publicly linked with crime, it seemed more and more reasonable for authorities to claim that someone using Tor or running a relay must be up to no good. The problem was that making a case for Tor in public was extremely tricky—you would get sucked into a quagmire, forced to condemn some use cases of Tor and promote others and articulate a clear vision of what the technology was *for* and what it was *against*. The delicate balance of the community made this even harder—many remained deeply suspicious of leaning too hard on democracy, human rights, or anything that could bring Tor closer to being a slick Western NGO.

The community responded in two different ways. One strategy, which emerged from the maintainer culture and would prove less and less effective as Tor matured, was to *publicly* do very little—to assert Tor's status as a neutral privacy technology and then retreat into the role of an infrastructure provider. This, at least at the beginning, gave the community enough cover to come up with clever hacks and legal loopholes to mitigate the immediate consequences for the network—hacks like setting up one's own internet service provider, or establishing a series of holding companies. These tricks would allow Tor to keep roots in as many communities as possible, growing the network without alienating those who might bristle at a particular political stance, or getting bogged down in running battles over ideology. This had worked for much of Tor's early life, reframing abuse as an administrative issue rather than a moral or political one, and appealed to the hackery sensibility of the operators, who were loath to get seriously involved in conventional politics, media work, or campaigning.

> I don't know, I'm quite averse to getting involved in policy issues. And I don't know if that's something that tech[n]ical people tends to share? They look at it and they go, oh, I don't really want to touch that, I don't like making rules and things, especially when I know someone's going to go through them and mess

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

them all up after I've written . . . I'd rather just implement a technical fix that prevents their law from being effective.

Core Tor contributor

I can innovate faster than they can legislate.

Onion service developer

Although this strategy was understandable to those steeped in the culture of the Tor community, for many on the outside it seemed utterly bizarre. It did have some tangible benefits, allowing Tor to appeal to an enormously wide community—including some rather surprising characters. While retaining his engineer sensibilities and continuing to work on Tor development, Roger Dingledine was doing his best to mitigate these threats to Tor by speaking directly to law enforcement, giving trainings to the FBI and others to show them how Tor could help rather than hinder traditional approaches to law enforcement that relied on investigation over mass surveillance.[42]

Underneath this strategy lay a second, rather more "engineer" idea—slowly extending Tor, through alliances and new projects, to become part of the internet infrastructure itself. This idea had been building since the earliest days of Tor; as engineers developed new technologies, they were modularizing those technologies, separating them into component features that could be turned into a set of standards and subunits that could be taken and incorporated into other technologies. The subunits could be as large as the whole network itself—creating interfaces to make it easier for services to use the network—or they could be as small as individual anti-tracking workarounds that browsers like Firefox could incorporate into their own code. Cultivating a *neutralized* Tor (as the maintainers wanted), with as diverse and large a set of communities as possible, would (in theory) help to maximize its capacity to be incorporated into other projects, eventually making Tor more like encryption—a technology worked into so much of the background of the internet and underpinning so many vital business and commercial interactions that it was no longer viewed as controversial.

Ultimately, however, neither of these strategies was doing much to hold back the tidal wave of backlash to Tor. Without a robust case for its own place

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

in the world, instead of a neutral technology, Tor came to be overwhelmingly associated with crime. ISP after ISP banned users from setting up Tor nodes, and politicians and the media continued to rage against the Dark Web. But a sea-change was coming in Tor's culture. Its activist constituencies, long separate from the core of the project, were becoming more vocal over the early 2010s, and would usher in a new era for Tor.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

8 THE ACTIVISTS

As the late 2000s and early 2010s wore on, throughout the rise of the Dark Web, a counter-current was developing within the Tor Project that would go on to radically change the organization and its place in the world. While Tor had been funded since 2006 by the general movement for digital democracy (or, depending on your politics, the organs of American soft power), it had generally maintained a cool neutrality to political ideas in its public persona, appealing to a wide variety of different communities, some of whom were already queasy about its reliance on US state funding. But as the organization took on more people in funding and activist roles, and new developers from the more politicized segments of the hacker scene, many of those working for the Tor Project sought to connect Tor more forcefully to the political movements that saw the internet as a frontline of global power.

In the late 2000s and the early 2010s, as public internet access and early social media sites continued to spread around the world, the goals of US digital power seemed to be reemerging from hibernation. Internet tech was continuing to move out of startups into a global context, and with it, so did the engineers and hackers who had been creating these technologies. From the rise of Anonymous to the dawn of social media, from Snowden to the Arab Spring, hackers and internet infrastructure were becoming key fronts of power. Suddenly, the political valence of hacking—and of Tor—seemed undeniable.

To trace the roots of Tor's growing engagement with political struggle, we have to go back to the start of its history. Across the late 1990s and 2000s,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the United States had, along with a range of NGOs (including Bridges.org, set up by Shari Steele of EFF), incorporated digital technologies into its aid and development programs. The aims here were twofold: to spread digital tech and literacy in developing nations, and to open up novel markets for digital services. The United Nations and the World Bank instituted a range of programs in Egypt, Tunisia, and other nations across Africa and the Middle East often focused on providing a combination of digital infrastructure and IT education for young people.[1] For the US government, this had strategic implications, presenting a possible regime of global soft power—and for many, a beneficent form of global capitalism, sustainable development, and potentially infinite economic growth.[2] An explicit aspect of this development was the idea of digital democratization—a kind of structural determinism that aligned well with an engineer's sensibility for a model in which open and flat networks for communication and commerce disrupted centralized societies and promoted freedom (and profit).[3]

As the 2000s progressed and internet access continued to spread, many governments around the world began to enact draconian measures—both legal and technical—to control what they saw as a dangerous and destabilizing extension of Western power. Far from inherently democratizing, the internet proved to be equally capable of embodying and empowering more centralized and authoritarian modes of social organization. The US' own attempts to embed law enforcement control over the internet's basic infrastructure and protocols had been fought fiercely by organizations like EFF in the 1990s; although law enforcement and media companies continued to push for control over the 2000s, the Crypto Wars had (at least in public) led to monumental growth in digital companies in the United States and Europe, which together formed a powerful lobby against overt centralized state control.

The authoritarian hold that governments like China and Russia were seeking on their domestic internet became a serious focus for US foreign policy. As it continued to spread its wings as an NGO, the Tor Project's new funders increasingly foregrounded its anti-censorship properties. To many of the anti-authoritarian techno-utopians of the internet freedom movement, the internet was not just a source of dystopian control—they saw within

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

it the potential for a global utopian society, to spread democracy. And so, despite their bitter domestic rivalries, the activist movement and Western state power began to find common cause on the global stage.

The cultural roots of a social movement around digital freedom and privacy were already well established, particularly in the activist culture of organizations like EFF. These groups—and the digital freedom movement more broadly—had long held a contested relationship with the United States. On the one hand, they were largely funded by public donations (although linked to an ecosystem of start-ups and think tanks) and closely aligned with the US geopolitical soft power goals of spreading democracy through development and digital technology.[4] On the other, they had long been deeply critical of US spying (both domestic and foreign) and had pushed back repeatedly against the US government's own overreach in the digital realm, through court cases, activism, protest, and political lobbying. Through the late 2000s, EFF and others would lend critical support to the promotion of the internet as a democratizing force on the world stage, with the movement as a whole absorbing vast sums of government money flowing into digital development.

The resurgence of Western digital soft power and grassroots anti-authoritarianism in the late 2000s continued to fill the tech ecosystem with money and new people, growing a much larger and more lucrative digital activist movement. The digital activist scene extended beyond the bureaucratic world of the United Nations and the few well-established NGOs, flowering into a dizzying array of start-ups, conferences, and activist organizations. The digital rights community was becoming a movement of its own, composed of alternative news sites, technology projects, activist groups, and lobbying organizations that were increasingly communicating and collaborating.[5] This planted the seeds of a radically new cultural counter-current within Tor, as it sought further money, support, and attention in the digital freedom movement. The sea change in the wider digital rights landscape connected the Tor community with people, often long-time fans of Tor, who were much more openly engaged in politics and burgeoning online social movements—and the money of the NGO sector.

Some existing members of the Tor community began to take up this wider mantle of cultural change. Jacob Appelbaum, a young developer and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

activist, had joined Tor in 2007, shortly after its establishment as an NGO and its early success in securing a more stable funding base from the International Broadcasting Bureau and Internews. In 2008, he was the only full-time paid developer on the books apart from Dingledine and Mathewson, though he was part of a growing team of volunteers and part-time contributors. Appelbaum had grown up in the hacker underground scene, having taken part in hacker groups like Cult of the Dead Cow that blended hacking with engagement in protest and politics. He also became the US face of Wikileaks, as its (at the time) only public-facing American member.[6]

As Tor's new funding and growing community focused on expanding its user base, it complemented improvements in speed and interface design with efforts to promote its use in activist communities around the world through talks and training events. Appelbaum spent a number of months in 2008 and 2009 touring the Middle East and North Africa, holding digital training events and presenting on Tor.[7] There, he (and later, other members of the core Tor team) showed groups of activists, civil society organizations, and students how Tor worked, what kinds of surveillance it might protect them from, and how to use it to evade online censorship and blocks put in place by their governments. Appelbaum quickly became the younger, more media-friendly face of Tor—happy to provide incendiary quotes to the press and get into public arguments with those making a case for online censorship or surveillance.[8]

My interviews with other members of Tor who joined around the end of the 2000s and beginning of the 2010s suggest that this was part of a pattern (one that they alleged stemmed from Tor's then executive director, Andrew Lewman) of young staff and contractors in their early twenties being dispatched around the world at short notice to be "at the scene" of major world events on behalf of Tor, often with little preparation or support, in situations outside their comfort zone and beyond their ability to manage. As the work, and its profile, ramped up, the demands on many of these contractors were intense—major updates early in the morning, last-minute frantic demands, and increasingly combative relationships between Lewman and the younger staff. But Tor was only continuing to grow in prominence, as hacker politics began to enter the headlines at an alarming rate.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

At the same time, the platform revolution was taking hold at home, incubated by another offshoot of the hacker underground that, in the 1990s, had sought to take the digital technologies and develop them into disruptive capitalist businesses. Following the huge injection of cash and subsequent collapse of the dot-com bubble, a second wave arrived in the late 2000s, with the advent of early social media. A range of these service-based social platforms started to spring up, taking a very old model of the internet based around user-generated content on forums, blog comments, message boards, and IRC, and building in networking tools that allowed people to more easily build links with one another and share content. As has been extensively documented, this came with its own business model—collecting reams of user behavior data and turning these, along with the network graphs of human connections, into grist for the mill of targeted advertising.[9] Huge amounts of funding again poured into these social media sites, which began to spread throughout the world, growing their user base and laying down their own parallel internet infrastructure of server farms and local hubs. Along with the digital development programs and digital rights defenders, the seeds of US soft power were being scattered across the world in the form of internet technologies.

In 2011, to many in the United States, these seeds seemed to bear fruit. Across the Middle East and North Africa, labor and protest movements had been strengthening over a number of years in many Arab nations, with an increasingly politically active youth and working class taking to the new social media platforms to organize and protest inequality and corruption. Economic conditions in the wake of the 2008 financial crisis and global recession were contributing to a ratcheting-up of tensions and protest, much as in the United States and Europe at the time.[10] In early 2011 in Tunisia, the suicide of Mohamed Bouazizi, a young market trader who set himself on fire to protest mistreatment by police and a government official, sparked a rapid intensification of political protest and marked the beginning of the Tunisian Revolution. The governments of Egypt, Libya, Yemen, and Tunisia would each be overthrown by their own citizens in mass popular revolutions over the next year; Algeria, Bahrain, and Syria would experience civil wars; and there developed further unrest in many more nations, spurred on by mass

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

public mobilization across the region.[11] Authorities responded frantically, with internet shutdowns and subsequent moves to block social media and news sites where activists on the ground were organizing and getting footage and stories out to the rapt world media.

Tor claims to have played an important role in the Arab Spring in a number of countries, particularly in Egypt, with descriptions of protestors in Cairo evading internet shutdowns and taking to Twitter using the Tor network to hide their communications.[12] The network metrics used to make this case in presentations at the time tell a more complicated story.[13] With some estimates showing more than a million people protesting in Cairo at the height of the revolution, Tor users in Egypt appeared to peak at only a few thousand. While it's of course entirely possible that Tor played a pivotal role in sustaining reporting from Egypt, and that a small number of organizers may have used Tor to share information through their wider networks, it's likely that any effect was concentrated around a small number of individuals rather than a mass facilitation of online resistance. Nonetheless, Appelbaum fairly quickly became a rock star on the global media stage, taking Tor around the world along with a compelling narrative—of digital privacy technologies at the heart of a global movement against authoritarianism.

A common refrain when I started this research was that social media platforms and counter-censorship networks like Tor had played a pivotal role in the Arab spring—both by hard means (providing access to technologies for organizing, communication, and privacy) and soft (showing people new models of society by granting them access to US media and broadcasting their struggles to a global audience). Much was made of the fact, discussed in diplomatic cables acquired and released by Wikileaks, that a number of prominent activists in the movements had received training from the US government-funded National Endowment for Democracy program and democracy-oriented NGOs, or had attended summits sponsored by social media companies.[14]

While it is impossible to separate out the distinct roles that different technological projects—from Twitter to Tor—or training programs may have had in facilitating these revolutionary movements, it is certainly true that the *digital democracy* narrative imparts a great deal of importance to

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the spread of Western internet projects throughout the Middle East. The mode of power imagined here mirrors that of the engineers, with disruptive technologies undermining hierarchical societies by imposing flat structures for communication, organization, and liberalization.

This narrative of technological determinism is a simplistic one, denying the history and agency of the people of these countries, as well as a host of other factors. It implies a long-contested *hypodermic* model, in which people can be injected directly with propaganda or technology, rather than engage with it in critical and complex ways. The deterministic narrative also ignores the spread of protests against corruption and authoritarianism in the West happening at the same time in 2011, such as through the Occupy Wall Street movement.

Conversely, several prominent accounts at the time and since—not least by the people who actually took part—argued that although these tools were taken up and used for mobilization, the actual roots of these revolutions were much deeper, stemming from complex historical and social forces, and from decades of coordinated action and movements by the people themselves.[15] Some of these too implicated the West—in rather different ways—through reactions to the catastrophic effects of the global financial crisis and successive waves of US interference in the region.[16] The analog mass media played a significant role as well—particularly Al Jazeera, which was coordinating citizen journalism on the ground and getting stories out to a wider international audience. The real links with social media were complex, it having allowed stories to be collected by much smaller numbers of people, but to spread internationally.[17] Although it may have played some role in organizing, much older technologies like mobile phones may well have been more decisive. In Egypt, the even older social and information networks of the mosques and wider civil society-—central spaces more aligned with the Muslim Brotherhood than the anti-Islamist government—played an enormous role entirely divorced from the internet. Much of the digital democracy work has itself since been re-evaluated with rather different eyes, highlighting the often misguided sensibilities of some of those involved in this work at the time.[18]

It's hard to argue that Tor's funding and activities don't implicate it as at least aligned with US soft power, especially in the early 2010s, when much

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

of that funding came from US state organizations whose foundational goals explicitly include the promotion of global democracy. But this isn't the whole story, and it in fact hides a much more complex internal culture. Despite the power of the US state narrative, many in Tor and in the wider digital freedom movement sought to support freedom struggles in the Global South without doing so under the banner of digital colonialism, instead seeking forms of international struggle grounded in solidarity. That said, this narrative—of soft, beneficent US colonialism through markets and communications infrastructure—was certainly important in organizing money and activity in the wider technical scene for some time before and after the Arab Spring. Still, its experiences of the Arab Spring profoundly altered how Tor was understood to fit into the global landscape of digital rights. Tor's developers had seen firsthand the tools being promoted by others—and the very weak privacy protections those tools offered—and were keen to make Tor an even better option for the next time a wave of revolutions swept through authoritarian states.

Throughout the early 2010s, the political life of hackers and hacking continued to evolve. Separate from this more professionalized activist culture, a range of smaller political movements were emerging from the hacker underground. Wikileaks, preexisting this wave of grassroots digital protest, continued to ramp up its activities through campaigns of leaks exposing the misdeeds of the US military apparatus. It too wasn't engaging in activism in the same sense as the digital freedom NGOs (though it did make appearances at some of the same conferences), but was increasingly animated by a deep hatred of US imperialism as the organization centralized around Assange.

As the early 2010s progressed, Appelbaum grew increasingly close with Assange, becoming the main (though never formal) link between Tor and Wikileaks. A loose and casual alliance was developing, particularly as Appelbaum traveled around the world teaching digital security, speaking at conferences, and promoting Tor.[19] This made Wikileaks a rather odd ally for Tor: while Appelbaum was contributing to a more vocal and activist side of Tor, in practical terms, it aligned closely with the liberal democracy, US soft power-based applications of Tor that were so anathema to the harder,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

anti-US values of Assange. The relationship between Tor and Wikileaks was not embraced by everyone in either organization but the two became friends and allies, as documented in Laura Poitras' film, *Risk*.[20]

This more activist Tor counter-current was still fairly diffuse in 2011 and 2012. The surrounding NGOs and more radical cultures remained mostly separate from the core business of the project, which focused on maintaining and developing code and infrastructure. While people like Appelbaum were increasingly identifying with and taking part in these more explicitly political activities, the project itself largely maintained a certain ambiguity in its politics. Although Appelbaum was articulating a punchy, oppositional politics similar to that of Wikileaks, the Tor Project still incorporated a wide range of different perspectives, making its case to funders as a softer and more liberal digital privacy NGO, and to wide and diverse hacker communities as a tech project that they could contribute to, hack on, and support through volunteering.[21] Meanwhile, Dingledine was selling Tor to a far wider public, as he continued to strategically engage with law enforcement and politicians through talks and presentations. For the organization itself, these activities were to grow the project, not change its direction—to find new sources of funding, open up new user groups, and try to mitigate some of the roadblocks to wider adoption being thrown up by law enforcement, other internet infrastructure providers, and the press. The Snowden leaks in 2013 changed that.

Edward Snowden's story has now been told many times in many different places by many different people—including himself. Working as a contractor at a company working for the US Department of Defense's National Security Agency (NSA), Snowden had high-level security clearance and access to reams of sensitive surveillance material and operational documents. Snowden had an enthusiasm for Tor even before the leaks—he approached the Tor Project as a supporter and claimed to have been running a Tor relay while employed at the NSA. It may be surprising that someone working for the security agencies could be deeply committed to a techno-libertarian, anti-authoritarian politics, but in fact this is more common than you might think—especially among the technical staff of agencies like UK's GCHQ and the NSA. In 2013, however, he would use Tor to rather different ends.[22]

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Snowden had become disgusted with what he saw while at the NSA: a fractured landscape of legions of contractors with access to top secret documents and surveillance data that extended far beyond what was permitted by US law, many of whom were allegedly abusing the US government's surveillance platforms to their own personal ends. Reaching out to journalists Laura Poitras and Glenn Greenwald in 2013, Snowden used the Tor network to pitch them his story, transferring hundreds of thousands of highly classified documents relating to digital surveillance programs by the US and its allies. As he hopped around airports, hotels, and the homes of supporters evading security services—traveling first to Hong Kong, then finally arriving in Russia—Snowden trawled though the documents with Poitras and Greenwald, pulling out stories and packaging them into a campaign of media releases. Over the following months, the *Guardian* and the *New York Times* would publish Snowden's documents, dramatically changing the face of the internet and its politics.[23]

These leaks showed that, following the attacks on the US in 2001, America's attempts to execute its War on Terror through military action and domestic policing had been accompanied by a vast, concerted campaign to reorder the internet's control landscape—to establish itself and its surveillance apparatus as the point through which most of the world's communication traffic would have to pass through. In what amounted to a global mass surveillance operation, the US and its allies in the Five Eyes intelligence alliance had launched a mass spying operation on the global internet, encompassing its enemies and allies alike. Unlike its soft power vision of its own role in the Arab Spring, the United States was exposed as maintaining a hard grip on the infrastructure itself—the king of the control points, dominating the topology of the global internet.

This remaking of the landscape of online control occurred at multiple levels of infrastructural power. Some of it involved subverting existing control points in the internet infrastructure—such as taps on the undersea cables connecting continents, or crocodile clips on cables in the major internet service providers of countries around the world. Other tactics aimed to dominate practice and policy—creating data sharing agreements with social media platforms and infrastructure companies (and in the process

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

highlighting the new status of social media platforms as higher-level control points in the internet structure). Other aspects involved international collaboration to circumvent *legal* structures, involving the US' Five Eyes allies and including a deal with GCHQ to spy on US targets constitutionally protected from mass surveillance by their own government.[24]

The contemporary era of Tor was shaped heavily by the Snowden leaks and their wider impact. The first effects were a vindication of Tor's need to exist. Real evidence was made public of a global spying operation focused on everyday citizens. The imagined *global adversary* from Tor's earliest design discussions—or something very much like it—was real. Paradoxically (as this is the very adversary that Tor can't do much to protect from), this led to an immediate surge in users and interest in Tor, not least because it featured in much of the subsequent reporting, including in international headlines. A slide from a secret NSA presentation hailed Tor as "The King of High Security, Low-Latency Anonymity . . . there are no other contenders to the throne." The leaks also revealed efforts within the NSA and GCHQ to exploit Tor in a presentation called "Tor Stinks."[25] In this presentation, the intelligence agencies discuss a joint workshop between the agencies to establish whether or not they could systematically break Tor. It had emerged, across a concerted week of hacking, that Tor was in practice far stronger a defense against security services than they had thought. Just as the early developers had predicted, the security services couldn't get more than a partial picture of the network even by setting up and compromising relays, and although they could selectively deanonymize some Tor users, they couldn't systematically break the network.[26]

Although by the early 2010s, some of the core team had been skeptical that Tor provided much protection against the vastly powerful US spy agencies, they did now have some evidence that they could at the very least be a serious nuisance to the NSA. This began a further shift in how they talked about Tor's design, foregrounding an economic logic in which new protections were considered on the basis of whether they could increase the "cost" to the adversary of deanonymizing someone. Although they could never hope to beat the NSA in all circumstances, if they could increase the unit cost of deanonymizing a person from pennies to hundreds of thousands

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

of dollars, this would have a serious effect on the *mass* surveillance that was clearly emerging.

The broader effects of Snowden's revelations extended well beyond the activities of the security services, reverberating in a range of unpredictable spaces and places and shaping the *culture* of a new generation of the internet's vanguard. That culture followed the techno-utopian narrative of the Arab Spring with a sharp counterweight, no less connected to politics and global activism, but with the United States and its technology platforms as antagonists rather than saviors. The groundswell of optimism brough forth by the rise of social media as a global force was turning to skepticism and alarm, as it came to be seen as a threat to rather than a champion of democracy. The very social media platforms that had credited themselves with liberating Tunisia and Egypt were revealed to have been conducting mass spying around the world on behalf of the Five Eyes nations, who used those platforms to spy on even their own citizens.

Snowden galvanized a generation of young activists into action.[27] The new generation flooded the institutions of digital freedom with energy, work, and new ideas, with many smart and passionate young people joining the Tor community or volunteering to help with the project in their spare time. Many of these people were younger and fresh from the NGO space, and others were already active in the Tor community but newly infused with an activist zeal and sense of purpose. More than the juicy snippets of palace intrigue and technical detail from the halls of power published in the leaks, it was the huge flood of new users, developers, campaigners, and relay operators that would go on to have a lasting effect on the Tor Project. The cultures those users brought with them, and their urgent, activist energy, were rather different from the dusty world of engineering conferences and cryptography symposia, and different again from the more traditional, scrappy techno-libertarianism of the underground hacker scene of the time. Their energy added to the already growing activist segments within the Tor Project, and contributing to a strong cultural world opposed to both US spying and also the internet platforms and their role in surveillance.

Although situated in the context of US digital soft power, this distinctively activist culture emerging in Tor wasn't restricted to a particular politics,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

or to those working in administrative and funding or public relations roles. Many were skeptical of, or deeply opposed to, US colonial power—the digital freedom community itself was an odd amalgamation of liberational, libertarian, and liberal movements. People in the wider Tor community were becoming more willing to see Tor as aligned with a wide range of other, often directly conflicting, political struggles—setting the scene for a battle over what sort of social movement Tor would actually support.

The Tor Project itself began to slowly make a number of moves to strengthen this growing organizational focus. As its funding and reach expanded, some of the newer crop of developers who had been joining Tor in paid positions were more willing to connect the structural politics of anonymity engineering to explicit political organizing and membership in social movements. The seeds of this shift had been planted before Snowden's revelations, as some developers and members of the relay community had already been active in political organizing and activism for some time. Part of this reflected the different kinds of work that these relatively new developers were engaging in—often attempting to bring in features requested by funders, such as improving Tor's counter-censorship or anti-tracking capabilities, rather than more abstract anonymity engineering. But this was also simply the social context in which this younger generation had learned to relate to their work, with protest movements growing across the United States and Europe and hacker communities increasingly stepping off the sidelines.

Isis Lovecruft, an anarchist activist and cryptographer, encapsulates one version of this new politics of Tor. Joining Tor in 2010, they brought a more explicitly political character to development work, combining their cryptographic research with discussions of anarchist political theory and the context of social movements and new civil rights struggles sweeping the United States. But, as is clear from their writing, they still had strong links to an engineer's view of the world, which, though different from,was not incompatible with an anarchist politics that was concerned with power written in social and political structures. Many more developers, whose politics reflected these wider changes in the hacker political landscape, would join the project over this period, such as Chelsea Komlo (now at ZCash and for a period a member of Tor's Board of Directors) and Erinn Clark (a developer at

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Tor and Debian, and also for some time a link between Tor and Wikileaks). They mostly couldn't be described as liberal in the same sense as the *digital democracy* people, with the new members generally espousing a more radical and anarchist-feminist politics, but together represented a new set of cryptographers and coders rooted in quite a different cultural environment than were Tor's earlier engineers.

Counterintuitively for a project funded by the US government, Tor seemed poised to become the technological jewel in the crown of a global digital freedom movement increasingly at odds with the US. The very movements, structures, and organizations that the West had been funding a handful of years earlier—in the interests of supporting popular revolutions in authoritarian nations—were turning their critical power and activist zeal back on the West. This period, accordingly, saw a further international turn in Tor and the Tor community. Although often represented as a US-based project, it had always had prominent members based in the UK as well as in Germany, where anti-surveillance hacker culture long held a profound influence on the international digital rights scene. Following Snowden's leaks, the networks of international digital rights activism drew in a wider range of people to Tor, from Italy, Spain, and other European tech scenes to Uganda, Cuba, and the Global South.

Tor's growth continued to accelerate: as one developer told me, when they started, wearing a Tor T-shirt at a conference had a real "cool factor" cachet, but as time went on even the core Tor community could fill a mid-sized venue, and Tor merchandise no longer turned heads. Newly formed projects began budding off or attaching, remaining under the protective umbrella of support offered by the Tor Project, but with a greater deal of autonomy. One of the most notable, which remains today an important contributor to Tor's broader role in the world, was OONI, the Open Observatory of Network Interference.

OONI had come from a new developer named Arturo Filasto, a hacker who had risen up through the Italian technical scene before meeting the Tor developers at the Chaos Communications Congress (a common story in the life of Tor). Filasto, who had long been interested in internet censorship, began to develop tools to measure government's blocking of the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

internet—and of Tor—as a volunteer. Working with Isis Lovecruft and others in 2011, coding amid the aftermath of all-night parties in smoky shared living rooms and on precariously perched laptops in airport waiting lounges, they turned a jumble of scripts and experimental tools into the OONI Probe project. The software could be used around the world by volunteers to detect censorship—to watch the watchers. OONI was set up in 2012 as a sister organization under the Tor umbrella and attracted its own community of developers and volunteers.[28]

Whereas Tor extends a volunteer network of relays around the world to carry and anonymize internet traffic, OONI turns that design on its head. It is also based on a worldwide community of volunteers, but OONI's network does something rather different—rather than speaking to the internet, it listens. Instead of relays, OONI's operators run probes—programs hosted on mobile phones, personal computers, and server racks that regularly try to access a variety of websites that are likely to be blocked by governments (though are generally not illegal). At the same time, OONI's own servers in the United States attempt to access the same websites, also recording what they get back. By comparing the two responses—the data returned by the website to OONI headquarters acting as an experimental control for the reading taken "in the field"—OONI can detect and map internet censorship around the world.

The data collected by OONI showed not only when and where the internet was being censored around the world, but *how*. It allowed the "openness" of the internet to be measured directly, providing key signals for journalists, for example, around internet shutdowns used by governments to suppress protest, as well as active intelligence for Tor on how it was being blocked. The OONI team were also early pioneers of Tor's outreach work in the Global South, growing out of rising concerns with internet censorship, particularly in the context of elections. As they traveled the world setting up OONI probes in countries that were censoring their internet, or that had upcoming elections, the OONI team began to develop links with activists on the ground, forming particularly strong connections in Uganda and Cuba (where they shot a short documentary). But despite its clever design, OONI doesn't change the landscape of the internet itself in the way that Tor

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

does—it instead maps how governments are trying to change this landscape themselves, supporting the work of activists and journalists to fight in the domains of law, policy, and public opinion.

During this time, Tor's developers were using the influx of energy, enthusiasm, and money to extend and transform the technologies of Tor themselves. Many of the newer developers were focusing their efforts on surveillance higher in the stack—not hacking on Tor's core design or crypto protocols, but on the browser itself, trying to find ways to subvert the cookies and trackers that social media platforms were using to track people. Tor began to work more closely with training organizations like Tactical Tech, which were continuing to hold digital security trainings for human rights defenders and educate about technologies like Tor, but were doing so increasingly for Western organizations coming up against the policies of US and European law enforcement.

Many of the technical innovations around Tor in this post-Snowden era related to journalists, who were a newly relevant group of potential primary users. The focus had heretofore been on journalists in authoritarian and nondemocratic countries, particularly in the Global South, but now anonymity was urgent to the Western press as well. The pressures that security services had placed on the *Guardian* following its publication of the Snowden leaks, the developing war against Wikileaks by the US and UK governments, and later the election of Donald Trump in the United States would bring home to many Western journalists the importance of anonymous communications. In this context, the SecureDrop project, entirely outside the Tor organization, would develop a set of technologies that adapted onion services into a vital new use case. A group of developers at Citizen Lab, led by Jen Helby, would work with a handful of early adopters in the mainstream press (notably the *Guardian* and the *New York Times*), taking the onion service technology and adapting it to the modern newsroom, allowing it to act as a dead drop for journalists where sources could securely submit leaks and anonymous stories.

> [journalists] are getting people to speak to them in a truly free way that they would not in almost any other context. You know, there's no . . . parking garage

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

where you can go to speak to, you know, Woodward and Bernstein any more, that's over. SecureDrop is that parking garage.

Onion Service developer

Some of the most important innovations coming from outside Tor came from even stranger parts of the digital ecosystem. Around this time, Alec Muffett, a developer at Facebook, did something radical. For Facebook, Tor's anonymity protections were of little interest, but its capabilities for circumventing censorship were potentially transformative. For the Web 2.0 and social media sites, for whom Tor had previously been a source of abuse, it now represented a way to broaden their user bases into a global community of nation-states—countries like China—that were increasingly trying to keep them out. This resulted in a small team at Facebook, led by Muffett, setting up a Facebook onion service in 2014 to allow people to evade state-level blocks and access the social network.[29] Rather paradoxically for a company now synonymous with surveillance, Facebook's onion service quickly became one of the most widely used applications of Tor, reporting a million users in its first year.[30] But the world's most notorious surveillance corporation buying into a privacy technology isn't actually a contradiction. Recall Chapter 1, in which privacy was understood as the demarcation of specific spaces of power; here, Tor separates Facebook's own spaces of power from those of national governments.

Shortly afterwards, Muffett released the Enterprise Onion Toolkit, an early step towards commercial standardization, that allowed an organization to easily set up an onion service by following a handful of fairly simple steps. Many legitimate services and sites began to set up onion services of their own. As more and more began to spring up from activist communities, an ecosystem of onion services—legitimate, stable projects run by mainstream organizations—began to develop. Taken together, these services, which spun up in this newer, more activist era, began to provide a counterpoint to the Dark Web narrative—giving the Tor Project something more concrete to sell.

Outside the fusty halls of the Privacy Enhancing Technologies Symposium and the warehouse raves and scrappy talks of the Chaos Communications Congress, Tor was moving into new spaces, dominated by international

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

NGOs, politicians, mainstream journalists, and funders. One of my earliest research trips for this project was to the Internet Freedom Festival, an annual gathering of internet freedom activists, held in baking-hot Valencia. Visiting the Open Observatory of Network Interference's stall at the conference, I was struck by the culture percolating through the talks and social events, and how different it was from that of the CCC. Although there were plenty of people there from scrappier hacker projects, the space was deeply infused with the aesthetics, values, and money of US international digital rights NGOs.

Following the Snowden leaks and subsequent influx of new members, the growing activist culture within the community developed a coherent privacy world centered around Tor. It became clearer what activism specifically around Tor would look like, how it would interrelate with other groups in the digital freedom space, and how this would all translate into changes in the technology itself—the features and user groups that it would prioritize. The sensibilities and priorities these new members brought from their previous lives combined with their lived, everyday experiences of trying to sell Tor—to fundraisers, new users, and policymakers—to bring together a new, stable privacy world in the Tor Project. As these ideas gained prominence and capital within the community, so too did this new culture of privacy. Along with the engineers' ideas of *privacy as a structure* and the maintainers' insistence on *privacy as a service* came a new and boisterous activist world—a world which saw *privacy as a struggle*.

The activist perspective saw Tor as more than a disruptive technical fix to the internet's landscape of power or a service provided to its users. It saw Tor as a social movement in its own right—engaging in the terrains of thoughts, feelings, ideas, and politics. Although the maintainers had asserted the neutrality of the infrastructure, arguing that "Tor is just a tool," the activists countered this. To succeed, Tor had to act in other domains of power. Engaged in movements beyond digital anonymity, such as feminist, antiracist, and queer rights causes, they saw the risks of other groups co-opting technologies like Tor: neo-Nazi cells using it to evade the police, politicians using it to justify controls on the internet, or Tor losing the battle of ideas altogether and being banned. Seeing Tor getting outmaneuvered or stymied in domains outside of the infrastructure itself—in the press and in

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

politics—they could see that to stay funded and grow they would need to wage cultural, legal, and political battles. Clever hacks and workarounds would only work for so long in the face of real political violence and repression. They were far more ready to engage in these fights, with resources, skills, training, and tactics, than the maintainers had been.

In the wider Tor community, the activist perspective bubbled up in diverse ways. For some, this replicated more or less the digital democratization argument, indistinguishable from the US State Department narrative:

> I think some Tor people maybe disagree with this view, but . . . so, one of the things that Tor gets its funding for is helping dissidents in countries with repressive governments. Like, Iran is an example. And . . . I actually agree with the idea of doing this, and it can sound a little, maybe . . . colonialist, and I see that point of view, but on the other hand we're not forcing anyone to use this tool. This is a tool for individuals and an individual anywhere in the world is allowed to use it, so I'm quite enthusiastic about, let's say, translating it into whatever language, Farsi or whatever. Localising it for people from . . . whatever country, and so that's part of our funding, and it comes from the US government. And I think it's a valid thing to do.
>
> Tor core developer

For others, this drew more on anarchist or feminist ideas. Within this activist perspective was a growing internationalism, which retained the desire to make change in the world, but which wanted this change to be driven by a community of equals in solidarity, rather than as simply a Western cultural export. But what these groups all shared was the idea that online privacy—and Tor—could be part of a bigger set of struggles.

This began to change how the Tor Project conducted itself. Engaged more fully at the sharp end of trying to "sell" Tor to the public and craft a compelling set of stories about it, for many of these people it became impossible to simply take a neutral standpoint on some of the things Tor was being used for. A new strategy was emerging more clearly—Tor was *for* some things, and not others. To the activists, Tor wasn't simply a neutral privacy technology that didn't care what you used it for; it was about journalism, freedom, democracy, and activism—embodied in the new services that were springing up and the new user groups it was trying to attract. This was a

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

far cry from earlier attempts to cultivate a more ambiguous politics that would allow Tor to be sold in very different ways to different people. But it proved useful in allowing it to counter the bad publicity of the crypto-markets and the Dark Web—Tor had a real, positive set of use cases which chimed with the evolving narratives around the internet as a new space for activism and social change.

> You need to be working out how to present the good use cases along with the bad ones. Um, I think they're still learning as an organisation how to do that, they've not really had to do that for the last decade, because they've had a bunch of government funding, and they've been able to tailor it to what they want to do. Now that they're more reliant on people and outside organisations for funding, well it looks like it's going to be that way, especially in the next few years, they have to get better at selling the technology as a whole to society.
>
> Tor Onion Services developer

Tor took further steps to counter the negative impressions that had taken hold. It hired a public relations company in 2014—Thompson Communications—to improve its image, initially highlighting the fact that, among the tech community, Tor was already pretty well integrated as a "digital citizen," engaged in collaborations with well-known projects like Firefox. Along with this, Tor began to build its own media team. The Tor Project was beginning to slowly drop the affectation of neutrality that had served Tor well in its early days, but was increasingly inadequate to meet the challenges it was facing.

The activist segments were gaining particular prominence within Tor—understanding privacy in the language of laws and liberal values, as a human right rather than a structural property or a service. By 2015, when Isabela Fernandes (formerly a product manager at Twitter) joined as Tor's project manager, this was a key part of the "glue" that attracted and bound many of the new people coming in. But even at this stage, there was still very little internal structure—which led to some problematic dynamics. Outside the core team, "Tor people" were largely employed as short-term contractors funded by grants. A number of core members told me that message discipline

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

had begun to break down, with different factions within the organization making their own pronouncements about Tor and its values in public. As one developer told me, this caused serious conflicts over Tor's values and public stances to rage internally—putting off many who wanted to shape the more value-centered case for Tor that was emerging, and empowering those who could weather these arguments to speak more freely.

Amid this growing turmoil, and (as some of my interviewees alleged) increasingly distant within the project, Lewman saw his position as director becoming tenuous. It was clear that Tor needed a change of direction, management that could better manage its complex place in the world and its heterogeneous community. In 2015, Lewman retired as Tor's executive director and the organization began to seek his replacement. Possibly nobody could have been better suited than Shari Steele to steer Tor into this new era. A veteran of the digital rights space—the director of EFF since 2000 and, since 1992, one of the central figures in growing it from a tiny group of advocates and lawyers into a highly effective lobbying and campaigning organization—Steele was also a long-time supporter of Tor. She was hired in December 2015 explicitly with a mission to further link Tor with the burgeoning digital activist and privacy movements.[31] Tentatively, she began to professionalize Tor and broaden its fundraising efforts, focusing on diversifying its donors and laying the foundations for grassroots funding drives that would allow Tor to move away from US government support.[32] Steele, and a range of new hires focused on professional services, developed Tor's already strong links with the digital rights activist movement, strengthening its connections to organizations like Tactical Tech, its lobbying and media capabilities, and its focus on usability, outreach, and training.

Engaging in power and politics had some consequences—especially for those more aligned with the anti-imperialist, radical side of the activist world. After reportedly being harassed by the FBI in 2016 because of their involvement in Tor, Isis Lovecruft would temporarily flee the United States to Germany, and Appelbaum would similarly report being detained by law enforcement in airports and questioned about his role in the project. [33]And the governments of the world were beginning to

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

counter Tor's efforts to circumvent their hold over their domestic communications infrastructure.

Blocking Tor is simple on paper—nations like China could simply query the directory servers for a list of the IP addresses of all Tor relays and tell their internet service providers to prevent all connections to the Tor network. In addition to blocking Tor in this way (which could be circumvented by bridges, secret relays run by volunteers that weren't publicly listed and could provide entry points to the network), Chinese censorship employed a range of mechanisms to profile Tor traffic based on characteristics of how it looked coming through the infrastructure. Tor responded with a technical solution in the form of the pluggable transports project—disguising Tor traffic to look less distinctive.[34] But Tor's political efforts also had real successes, genuinely changing how Tor was talked about by a media that increasingly saw its utility. Journalists were far more likely to see the lighter side of the Dark Web if they or their colleagues ran a service on it.

As these successes mounted, the cultural fault lines within the Tor community had never been more apparent. Tor was now a heady mix of military-academic-crypto people from the old days, most of whom could have emerged directly from 1960s MIT labs, classic hacker communities steeped in Cold War German counterculture with a libertarian distaste for "movement" politics, and a newer generation of hackers, managers, and fundraisers who wanted to take Tor to the frontlines of the political struggles of the time. This group themselves were not homogeneous—a mix of sharp, professionalized NGOs and activists, cool anarchist feminists, and the edgier Wikileaks-aligned people like Appelbaum.

Tor's increasingly value-oriented stance met fairly serious resistance from some within the relay operator community. Some pointed out that it was bizarre for Tor to condemn neo-Nazis using its network when it had been largely silent on the documented issues of child abuse. Some of these arguments are more justified than others. It is fair to say that much of the negative reaction to the activist turn in Tor was motivated by a reactionary queasiness towards feminism—in particular by some in the wider relay and Tor supporter community. This conflict is by no means limited to Tor, and was part

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

of a wider reaction by proponents of older and more libertarian components of hacker culture to the flowering and diversification of the hacker scene.

> This changed to, Tor is now about women's rights as well . . . They are probably right, with everything they say, so don't get me wrong. But Tor isn't specifically about empowering women and technology. I mean, they can do that, whatever. Take turns, do workshops, whatever. But that's not why I'm running a Tor relay. I'm running a Tor relay because there are people in Turkey and they're in jail for things they write, because people in Syria are getting killed if they are found reporting from certain areas. People in China just disappear if they are found using Tor, that's why I'm running Tor relays, Tor bridges. That's what I care about. Women's rights—fine, but, just, sorry, not my department! And saying that out loud makes people upset.
>
> Tor relay operator

But this is not to say that all criticisms of an activist Tor were entirely anti-egalitarian or animated by reactionary sentiments.[35] The articulation of a more explicit politics, allying Tor with freedom of speech and other liberal values, has some real practical consequences for the relay operators themselves. The design vision of the relay network on which Tor relies necessitates a wide distribution of Tor operators and users throughout the globe. This poses serious issues for relay operators in non-democratic countries, who can face real issues if Tor's implication in US soft power comes too far to the fore.

Before, Tor retained enough "productive ambiguity" around its values that an operator, user, or advocate could frame a wide range of different arguments about its value—selling it, for example, as an anti-corruption tool, a law enforcement investigative technology, or an innovation in security standards depending on whom they were talking to. However, by bringing the picture of Tor's values and politics into sharper resolution with rhetoric about freedom fighters, promoting democracy, and countering censorship, the activists who were selling Tor in the language of Western NGOs were making it easier for governments around the world to frame it as a Western colonial export and a tool of US soft power. Equally, some of the existing community had issues with the slicker NGO culture, which they saw as anathema to the anarchic and joyous chaos of the different hacker

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

communities in which Tor had its roots, and were uneasy about the potential that Tor might be co-opted by a savvier, more media-trained and policy-focused community in service of the US digital activist scene.

> I think that there's a trend in the internet freedom community towards legislative solutions to problems . . . or at least a reliance on them in ways that I don't think is appropriate when you're dealing with nation state adversaries . . . a large chunk of the internet freedom community [is] almost solely focused on those issues rather than focusing on technical wins.
>
> Onion Service developer

The growing activist world was developing a dialogue with the engineer culture, somewhat in opposition to the proposed "neutrality" of the maintainers.

> But the act of [running a Tor node], just like the act of creating an internet service provider where there wasn't one before, is a political act, right? It changes the landscape, and the relationship between people, and what people can do, and can't do, you know, so it's, I mean, yes, it is [political] . . . People who say that the choice to do this is not political are deluding themselves.
>
> Tor relay operator and activist

Although the maintainers' neutralized form of politics had managed to coexist rather well with the engineers' focus on structure, a new detente was emerging. Many of the engineers, particularly the newer developers, increasingly had a foot in both worlds—working these ideas of movement politics, human rights, and political activism into their own more structure-focused ideas about online power.

As the organization approached the mid-2010s, the loose and increasingly uneasy alliance between the different cultural worlds of Tor was beginning to show strain. The Tor Project was still trying to keep all these perspectives in balance, but it was becoming clear that this couldn't last forever. These conflicts and new alliances set in motion cultural changes that—when combined with increasingly untenable internal dynamics—would nearly destroy the Tor Project entirely.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

9 FACING WORLDS

For several years, the three *privacy worlds* of Tor existed alongside each other quite well, the tensions simmering below the surface. But, as the wider world shifted around them, these internal tensions came to a head. In this chapter, I discuss the events that caused this conflict to surface, how Tor survived, and the radical transformations of the worlds of Tor that resulted.

The Tor community was primed for conflict as the aftershocks of Snowden's leaks reverberated around the world in the mid-2010s. The wider hacker underground was struggling to make sense of its own role in the world, trying to cope with the growing political importance of their chosen craft. This diverse international subculture had long been united by a love of technology, but was increasingly divided by their politics. And the money, fame, and opportunities that came with this new prominence of hacking on the world stage were beginning to reshape their communities.

Hackers had always had their folk heroes—gaining reputations from technical proficiency, high-profile encounters with the law, self-mythologizing, or creating a new widely adopted technology. But now, drawing money and legitimacy from the growing professional security community, from start-ups and corporate giants, from publicly funded activism, and from long-standing but newly cool academic fields associated with hacking, a number of "rock stars" were beginning to emerge—community leaders that presented a public face to a rapt international media.[1] Tor was no different, caught between a newly activist sensibility and a heterogenous techno-libertarianism, and trying to navigate a world in which some of its

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

members were becoming celebrities—particularly Jacob Appelbaum, who many within Tor felt had grown to dominate speaking engagements and the character of Tor's public voice.

But the combination of money and media coverage streaming into digital activism, along with increasing interest in disruptive tech more generally, meant that serious problems began to fester. The hacker underground had its #MeToo movement, in which it tried to reckon with sexual exploitation and the concentration of male power, earlier than much of the rest of the world. In Tor's case, this would bring the contradictions between the activist and maintainer worlds into full conflict, and signal a sea-change in Tor's place in the world.

In 2016, a group of Tor developers and members of the community launched a website with the address www.jacobappelbaum.net (now defunct). On this website, this group alleged that Jacob Appelbaum, by this point a core Tor developer and one its main representatives to the media, had conducted a campaign of abuse within the Tor community. Each story on the website—some anonymous, some named—documented a person's professed experiences with Appelbaum. They ranged from accounts of intimate partner abuse, to Appelbaum taking credit for the work of others, to bullying and harassment across a span of more than five years and in a number of the communities surrounding Tor, like the Chaos Computer Club. In the parties, conferences, and workplaces of the global digital freedom scene, they alleged, Appelbaum had used his rising fame to cement a long-running campaign to centralize power around himself, to take credit for others' technical work, and to engage in manipulation, abuse, and sexual assault.[2]

Although the charges they leveled were extremely serious, many of Appelbaum's accusers had good reason not to rely on law enforcement, and a grounding in anarcha-feminist politics that preferred community-based solutions over criminal justice systems that they saw as violent and illegitimate. The group claimed to have approached Appelbaum directly rather than having gone to the police, offering him the opportunity to engage with them through a professional transformative justice mediator. According to this group's account, he rejected their offer and the group then published their stories on the website. A number of things happened in quick

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

succession. Several members of the core Tor community went public with allegations about Appelbaum in the following weeks. An extensive account by journalist and hacker Violet Blue detailed what they described as a long-running pattern of narcissistic and violent behavior by Appelbaum.[3] This made international headlines well outside of the security and tech press, with major pieces in the *Guardian* and the *Washington Post* among others.[4][5]

The Tor Project had dragged its feet on earlier reports about Appelbaum, with Karen Reilly, the development director, having reportedly accused Appelbaum of abusive behavior in 2015 only to be herself accused of "spreading rumors" about Tor, and then subsequently leave the organization after both her and Appelbaum were given ten-day suspensions.[6] However, this time, under Steele's leadership, and with an overwhelming number of core developers and contributors within the community publicly attesting to the accounts against Appelbaum, Tor acted. The Tor Project formally suspended Appelbaum while it employed a private investigator to substantiate the accounts, then ultimately expelled him from the community entirely.[7] The Chaos Communications Congress, The Debian Project, and the veteran hacker outfit Cult of the Dead Cow would follow suit in banning him from their communities. Appelbaum, who denied the allegations, stepped down from Tor and largely withdrew from public advocacy work thereafter.[8]

A deep fracture opened in the wider Tor community. For the majority of people working for the Tor Project, it was clear that addressing wider issues of misogyny and sexual harassment had become an unavoidable moral imperative and necessitated serious changes in how Tor functioned as an organization. Tor could scarcely claim to be a positive force in the world, or represent values of social justice and collective struggle, if it overlooked abuse internally. While not a "structureless" community, Tor had long been a self-described *do-ocracy*, with individuals having a great deal of autonomy in their own work. It had become clear to many that the informal ways that the community had been regulated needed to be formalized.

> I think these organisations come together, and there's all this idealism, and things that come in. And then there's personality types that, not necessarily trolls per se, but . . . where the, the goal is much more, sort of, self-centred, that kind of undermine the original ideals and things, but because by its nature it's,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> sort of, open and accepting, and then they basically, it doesn't take many of them to break the organisation apart. Unless it has, sort of, structural things in place, and has community management and HR and whatnot, so that that's less likely to be an issue.
>
> Tor core developer

However, the Tor community was split across this cultural divide. Most, particularly those who had devoted years to the Project, were in favor of the action it was taking against Appelbaum, supported by overwhelming testimony from a wide range of people in the hacker and digital rights communities in which Tor had its roots. However, the mailing lists and comment sections featured numerous dissenting voices who saw the treatment of Appelbaum as unfair. This minority decried what they saw as the consolidation of a long-awaited move towards professionalization and overt value-politics. One of several relay operators I spoke to said:

> Three years ago I paid a hundred Euros for getting a supporter T-shirt, which today I would be ashamed to wear.
>
> Relay operator

Although this conflict was nominally about the alleged actions of a single developer, it was clear that the fault lines ran far deeper. For years, Tor had managed to balance a wide range of directly competing understandings of the core meaning of the project, in an anarchic and diverse community. But, as the wider politics of hacking and digital freedom changed on the global stage, Tor could no longer sustain these contradictory understandings of its place in the world. Some drew a link to similar accusations against Assange in 2010—Appelbaum had also been involved in the Wikileaks project, and a minority saw the actions taken against him as an external attempt by shadowy forces to undermine their favorite developer and crypto-media personality.[9] But there was still a sizeable contingent who, despite what they might have thought about Appelbaum and the accusations against him, had serious qualms over what they saw as a shift to a more professionalized, liberal, and activist identity for Tor. In terms of our biography of Tor, it's clear that this battle between the maintainer and activist worlds might at one time have had the potential to destroy it, tearing the material base that

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

underpinned the technology from the ideological project needed to sell it to the world.

The Chaos Computer Club was itself convulsed by a similar set of issues, with rifts growing between the crustier, more techno-libertarian hackers and the new guard of politically engaged communities, some of whom were not themselves involved in activism but simply wanted to experiment with technology like everyone else without facing the misogyny and cliquishness that had long been a problem in hacklabs and open-source projects around the world. Posters for feminist hacker meet-ups clashed with posters decrying codes of conduct in the toilets of the CCC's cavernous conference halls. Online, arguments raged, with a wave of pieces decrying a culture of abusive "rock star" developers infecting the digital rights and hacker scenes.

While those arguments took place, those most vehemently opposed to Tor's response and its new direction largely left the project or dialed down their involvement. Localized mostly around the relay community, this miniature exodus did shrink the relay network for a few years, but it didn't have a direct effect on the technical side of Tor. In other open-source projects, the fissure might have created a *fork,* in which a group breaks off to develop the codebase in their own direction. But instead, there was little evidence of a technical split in Tor forming, aside from a few embarrassing splinter groups like the "Or Project"—an identical fork of Tor created by a small group on the periphery of the community, which purported to be "Tor without politics." They claimed to be working towards solving some of the basic design issues of Tor, problems that the world's cryptographers had been puzzling over for decades. In practice, most of their efforts went into changing the logo and the project fizzled out without issue. As many in the community would doubtless argue, the longer-term effects on Tor's technical development from the changes were the stemming of what had become a slower, quieter exodus of talented developers (particularly women and non-binary people) and their ideas and contributions from the community over the previous years.

Shari Steele, the relatively new director of Tor at the time, steered Tor through this period, overseeing a process driven by the board and many long-standing members of the Tor community and resulting in sweeping

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

organizational changes within the project. These changes consolidated what had been a number of years of slow movement toward a more professionalized structure for Tor, and were widely regarded by those involved most closely as positive. The first step was the election of an entirely new board of directors—the previous board had resigned en masse in order to support a fresh start for Tor. With the new board came a range of changes to some of the fundamental principles driving work in the Tor Project.[10] While for many years, Tor had exercised a light touch in coordinating the work done by its developers and volunteers, Steele, the new leadership, and many of those who had driven this change made it clear that they saw this laissez-faire approach as at least partly to blame for the crisis facing Tor.

In some ways, these changes were driven as much by economic imperatives as cultural ones. Tor's funding had historically come mostly from a few reliable central grants given by US government bodies, bodies that were often referenced by Tor's supporters and detractors alike. The regularity and stability of these sources meant that the organization had always enjoyed a great deal of flexibility in the kinds of work it could do within its core goals, and some leeway in how this work could be organized. Work on Tor, though reliant on a few core paid developers, could draw from an army of volunteers, passion projects, and others in the wider Tor community.

However, in recent years, more of Tor's funding had come from industry or private donations. The increasingly effective fundraising arm of the Tor Project had won a number of successes, in addition to major drives with the public, winning funding from a wider range of bodies like the Media Democracy Fund, the National Science Foundation, the Digital Defenders Partnership, and the Freedom of the Press Foundation. Although some of this funding, such as the NSF or Digital Defenders grants, was squarely from within the traditional US government streams of income, other funding was reliant on more actively promoting a particular set of Tor values, not least in order to distance itself from the Dark Web image that generally turned off funders and institutional collaborators.

Some of these new funding streams were more specific than those for "keeping the lights on" from US government grants, and often served to

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

advance specific technical or user goals: improving speed for users, translating Tor into new languages, or developing better ways to allow access in places where it was censored. And with more funding came more rigorous requirements—funders demanded regular reports on progress toward specific goals, proper human resources and project management procedures, annual reports, and stable financial management. Although the Tor Project had been required to do this in the past, this project management had often been left up to developers or done on an ad hoc basis. The new Tor looked very different from its roots as a small open-source project, from the anarchic assemblage of hacker communities that it had grown into, and from the oppositional, secretive, and centralized "citizen secret service" of Wikileaks. It was now becoming a more professional organization—and a more powerful one.

For some of the volunteer developers, the practical changes to the Tor Project didn't fit with the scrappier, more anarchic style that they had been used to. Previously, Tor had operated much in the model of the thousands of free software projects before it—if you had an interest, you could hack on it for a week or two, develop an archipelago of small side projects (half of which might wither on the vine), and then once every six months blitz out a fortnight of solid fifteen-hours-per-day coding, working up a tool or feature that would become a fixture of the wider Tor ecosystem. But now, instead of bursts of frenzied 3 a.m. Club Mate–fueled[11] activity followed by months of inaction, these grants required regular progress reports, administration, and a human resources department. [12]

> And then with the Jake fallout and different conflicts . . . a bit of the dynamics changed . . . I mean Tor is trying to become a professional NGO. Tor Project Incorporated. And I think that's a change over the previous idea of being deeply rooted in a lot of different communities. When you want to become a professional NGO, you have to make decisions . . . Before, you can be very flexible, and in different situations with different people act very differently. And it's not necessarily that there were any mistakes, it's just the growth is now changing things. And also, of course, changing who . . . stays around and what their incentives and motivations are for still hanging around and doing this kind of work.
>
> Tor core contributor

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

This newer crop of leaders had seen other organizations fall apart due to mismanagement and had little romance for the *burned out genius* model, which they felt restricted the pool of who could contribute and shape the project to a small set of rock stars, rather than a much wider community of different voices and ideas. They instituted a range of structural tweaks to how work on Tor was organized, including proper contracts and regulated working hours for core staff, and created a more equitable division of speaking roles at conferences to prevent one person from becoming too prominent amid the wider team. In some ways this was a deliberate move to a smoother, less exciting operation—more of a traditional NGO. It also, however, made sense in its own way as a pitch to the engineers—decentralizing the social structures of power that had undeniably accumulated within the network of people working on Tor.

This was only thrown into sharper relief in 2016, with the shock presidential election of Donald Trump in the United States. A pivot away from state funding now seemed imperative, both to ensure that a leader they perceived as erratic and authoritarian would not pull the plug, but also to avoid the association with the US government itself. Tor began to court private donors in earnest, ramping up a crowdfunding model to diversify its funding base, which also grew the organization, attracting developers and new projects and alliances drawn to a Tor that was more eager to join the frontlines of digital freedom.

It's no secret that Appelbaum's departure and its aftermath radically changed how Tor functioned as an organization. But the wider cultural change in the community that resulted—the balance between the worlds of the engineers, the maintainers, and the activists—was just as important. Tor's internal cultures had been changing for some time, but the departure of Appelbaum was a catalyst that locked in these changes and resolved some of the internal contradictions that had been growing.

The activist world, which saw Tor and online privacy as part of a social movement, grew to dominate the public face of the organization, reflected in a far more muscular defense of particular users and use cases. But this was closer to the culture of a value-centered NGO than to the abrasive and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

chaotic world of Wikileaks. This world was far from the "technical fix" idea of engineering solutions to digital power, of restructuring the world through clever applications of design and technical skill. It was clear that Tor, like most decentralized systems, relied as much on selling a vision—of privacy, of the future—to a diverse community of people around the world as it did on feats of engineering. The developers and the board began to articulate more forcefully, in the media and in their own communications, a core set of Tor use cases and values, bound up in a concrete vision of Tor's place in the world.

The Tor Project began work on formalizing this set of values and politics in a coherent statement, which retained the techno-libertarian roots of Tor and its foundational values but placed a much greater focus on human rights. This became the Tor Social Contract, published in late 2016.

1. We advance human rights by creating and deploying usable anonymity and privacy technologies.
2. Open and transparent research and tools are key to our success.
3. Our tools are free to access, use, adapt, and distribute.
4. We make Tor and related technologies ubiquitous through advocacy and education.
5. We are honest about the capabilities and limits of Tor and related technologies.
6. We will never intentionally harm our users.

Tor Social Contract (condensed), August 2016

Some of these values codified explicit aspects of Tor's social design: openness, decentralization, usability, and a commitment to free software. Others articulated more clearly a shift to centering values in Tor's work, more explicitly aligning Tor with the promotion of human rights, with advocacy work, and a future in which it could use its substantial influence to make political interventions. *Privacy as a struggle* was fast becoming a core principle within the Tor community.

> We are not just people who build software, but ambassadors for online freedom. We want everybody in the world to understand that their human rights—particularly their rights to free speech, freedom to access information, and

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> privacy—can be preserved when they use the Internet . . . Our vision of a more free society will not be accomplished simply behind a computer screen, and so in addition to writing good code, we also prioritize community outreach and advocacy.
>
> Tor Social Contract, August 2016

The new core principles were combined with a new strong public stance about what Tor *wasn't*. It was no longer anathema for the Tor Project to decry particular groups of users, to call out prejudice within its own community, or to moderate discussions on official Tor blog posts. Tor began to take strong positions when illicit or controversial use cases were reported; if you were using Tor to buy drugs, or to fund the far right, you weren't using it for its intended purpose.

> We've heard that the hate-spewing website Daily Stormer has moved to a Tor onion service. We are disgusted, angered and appalled by everything these racists stand for and do . . . Tor stands against racism and bigotry wherever and whenever such hatred rears its ugly head. It is our work to provide everyone with the best possible security and privacy tools so human dignity and freedom can be promoted all over the world.
>
> Tor Project Blog 2017

Some of this took a while to bed in, leading to misfires as Tor built up its confidence in the newer approach. In a now-infamous talk at DEFCON in 2017, Roger Dingledine, hair pulled back in his trademark ponytail, forcefully argued that not only was the Dark Web problem completely overblown by the media, it didn't really exist at all:

> There is basically no Dark Web. It doesn't exist—it's just a few web pages.
>
> Roger Dingledine, Defcon talk 2017

It's fair to say that this backfired—much to the dismay of some in the community, to whom it seemed a bizarre intervention when most of the world still knew of Tor through reporting about cryptomarkets. Despite this, Tor's new strategy began to win some real successes, especially as it finessed its messaging and came to recognize the harms associated with its use while promoting itself as a technology for journalists and human rights. The changing

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

US political context also played a role here. The election of Donald Trump in 2016 led to an explosion in interest in onion service technologies like SecureDrop, which rapidly expanded from a handful to more than fifty newsrooms around the US. Tor's utility for journalistic work took off, and the world's press increasingly presented a more "balanced" argument for Tor.

As one might imagine, the "it's just a tool" maintainer culture had a rather shaky place in this new era of Tor. But the relay network—and its culture—had been changing for a number of years. For some time, the network had been moving from an "atomized" model of relay operation, in which it was a libertarian community of anonymous participants, to a more collaborative maintainer culture, based around in-person operator meet-ups and a shared sense of purpose.

> And then there's also this element of, we should all get to know each other, because we're kind of in this boat together. Uh, even if we disagree on a lot of things, like, there's clearly something that's binding us together, so we should at least meet and talk about it.
>
> Relay operator

This was not least for security reasons. Over the late 2010s, the "bad relay hunters" were gathering increasing evidence of operators stealthily joining the network, setting up large numbers of relays behaving suspiciously, and potentially gathering data for security services. As the Tor Project tried to fight this, it gradually brought in much more regulation around who could contribute, as well as an expectation that operators would participate in local meet-ups, mailing list discussions, and the social life of Tor. The work of maintaining a relay had remained the same in theory, but professionalization at the core of the network meant that, although there would always be a place for the wider community, joining as a small operator was becoming much more a statement of support for Tor's movement than genuinely becoming a load-bearing part of the infrastructure. Outside the core super-nodes that processed much of the traffic, smaller, newer relay operators were mostly serving to add diversity to the network and to promote Tor to their internet service providers—work in the terrain of ideas rather than infrastructure per se. Although Tor had "designed in" a model of social organization to its

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

relay network, this was changing and evolving, even though the technology itself remained the same.

While it's clear how changes in its privacy worlds might shape the strategic moves Tor makes as an organization, who chooses to join up as a volunteer, or how other actors—law enforcement and politicians in particular—engaged with them, the *technical* consequences of such a culture shift might be less clear. A nuanced, more activist construction of *privacy as a human right* might well shape how Tor talks about itself, who it markets its technologies to, or who it asks for funding, but one could argue that engineering is a more practical business. However, the shift to a more value-driven approach changed the technologies of Tor as well.

The character of Tor's technical development—and the engineer privacy world—was evolving in important ways over this later period. The wider environment in which Tor was being developed was shifting, as an escalating series of leaks from the heart of power was opening up visibility into the innards of the US security state. The first hints of this followed fairly directly from the Snowden revelations. Snowden's documents had direct technical consequences for Tor—for one thing, it proved the real existence of the fabled *global passive adversary* that had haunted Tor throughout its history. However, the following years, in which information about the technical capabilities of Western spy agencies continued to leak into the public realm, pushed them further into action.

An example of development work from this more recent era of Tor shows a remarkable change in practices compared to the earliest design discussions of Tor in Chapter 4. In that earlier work, Tor's engineers had been evaluating defenses to theoretical *timing attacks* by a global adversary that could see the whole world's internet. Although they had dismissed these at the time, Tor received news in 2015 that the US government might have been attempting to collect exactly the information necessary to perform these timing attacks on Tor users.

The alternative media site BoingBoing had been running a high-traffic Tor exit node for several years, and, according to a post by Cory Doctorow on their site, received a subpoena from the FBI, asking them to "testify before a federal grand jury in New Jersey, with all [its] logs for our Tor exit node."[13]

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

In a since-deleted comment on this story, a university-based exit relay operator related their own experience of being subpoenaed by the Department of Homeland Security to produce three months of records for the IP address of their Tor exit node. This indicated to the Tor developers that these "netflow" logs commonly collected by internet service providers were being actively sought by law enforcement in the US:

> I would expect most US universities to be logging netflow in the very least. Even if the Tor operator isn't keeping logs, it seems safe to assume the network operator is.
>
> Developer, Tor-dev mailing list, 2015

Netflow logs are administrative records collected by internet service providers from routers. They provide timestamps for activity, indicating when a router is inactive and when it is sending information. This can be particularly damaging for Tor, as information on the timings of signals sent to and from Tor routers is exactly what is needed to perform the correlation attacks imagined in the padding discussion. In terms of our Cold War metaphor, this would be like a spy agency who has paid our agent's neighbor to monitor when they leave their flat—timing when they enter the Tor network.

> I think for various reasons (including this one), we're soon going to want some degree of padding traffic on the Tor network at some point relatively soon, and having more information about what is typically recorded in these cases would be very useful to inform how we might want to design padding and connection usage against this and other issues.
>
> Developer, Tor-dev mailing list, 2015

The developers asked the mailing list for any expertise—from people working at internet service providers or with experience dealing with netflow capture in another capacity—about the technical details of these collection mechanisms. This call for help collected a fantastic level of mechanical detail, down to the variation in the lengths of netflow timers in different router models, and the precise formats in which the records were stored. The developers, by mapping this information, realized that they could reduce the resolution of this timing information substantially at a very low cost by

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

introducing a small amount of *netflow padding* traffic into the network. This meant that the internet service providers, instead of getting timings down to the second, would get them in much larger blocks, which were useless for timing attacks. In our metaphor from previous chapters, netflow padding makes the difference between an attentive neighbor who records exactly when our agent leaves their flat to meet their source—at 2:32pm—and one who can only see that they left sometime in the afternoon.

The developers used attack brainstorming practices similar to those used in 2002—namely putting themselves in the shoes of dozens of potential adversaries—but now had real, material intelligence about what their enemies were doing, in stark contrast to the much vaguer picture of "The Man" they imagined in 2002. The developer in charge of leading this discussion designed an initial padding implementation, and then uploaded it as a patch in progress. Then something very interesting happened. Dingledine, still the lead developer on Tor, suggested that this could be taken as an opportunity to explore broader padding schemes for Tor, revisiting the earlier design discussion in its entirety and possibly making a fundamental change to Tor's threat model. However, the younger developer pushed back, saying that this fix should be restricted to a specific, small-scale change designed to thwart this particular attack. They argued that, as interesting as an abstract discussion of security theory might be, the implementation need for this minor, high-level feature to be plugged in directly outweighed getting bogged down in changes to the fundamental design principles of Tor. Following this decision, Tor then included a limited form of padding traffic for the first time—but the core design remained the same.

This discussion revealed a subtle but important change in the framing of privacy within the engineer world. The kinds of work here were very different—redesigning higher level features of Tor to counter a real attack, rather than abstracted attack forms based on the network structure As the knowledge and intelligence available to Tor's designers had changed, so had their approach to development *and their understanding of privacy*. As a result, design shifted from breaking down abstract categories into hypothetical patterns to instead engaging with specific mechanisms of surveillance (and hence specific adversaries). This new perspective still understood privacy as

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

topological power—embedded in the network structure—but in a much less abstract way, using the wealth of intelligence and data becoming available to them to map in finer detail how both the attackers and the users experienced this topology. Not all of this was due to the Snowden revelations; part of it was simply that Tor had become a more mature infrastructure, and so its design and development work had more data to work with and had increasingly built new layers and functionality on top of the initial, abstract designs.

Tor was now nearly two decades removed from its days as a theoretical framework, a test implementation, or a toy played with by some early adopters. The real advances in security at this stage were often piecemeal, but no less vital. The security services were more likely to deanonymize a Tor user through a tiny bug in Firefox's code or a tracking cookie than a fundamental compromise of the Tor design. So to counter these attacks, the developers had to comb through thousands of tiny parts of the programs and tools that Tor relied on, looking for anything that could be exploited.

> It started with a very simple idea of the Tor network. OK maybe that's not super simple, but at least you can describe the idea in a few sentences. But then the resulting work, you know, they have dozens of people working on it over many years, and it turns out that you don't just have to fix the network, you also have to fix the browser in many ways, because even though the network is . . . protecting your privacy in one way, that doesn't help if you're not protecting privacy in all the other ways it can be lost.
>
> Tor core developer

> That's kind of the thing about privacy is that it's like you're securing a house, right? And you have to lock all the windows, you can't just lock some of the windows [*laughs*]. Um, so that's where the kind of initial design is not enough, because we have to constantly be going through and looking for, what are all the privacy holes, what are all the problems? What are all the sort of, like, corner cases and so on.
>
> Tor core developer

This may also be one reason why some contributions to Tor have been lost or papered over, and some prolific contributors to Tor remain more or less anonymous—the media has often been less interested in developers

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

doing this kind of higher-level work if they aren't also hanging out with Julian Assange. The maturing of these structures itself was leading to a separation of kinds of work, with Tor's long-standing *do-ocracy* adapting to a more professionalized environment. As development work became increasingly specialized, trust within the core team—not only assured through technical means and community design, but through shared values—became more central to Tor's security.

> I guess that's where the values come in, because, you know, we have to trust eachother, that we're all doing the right thing in each detailed case. I mean I don't follow every ticket on our ticket tracker, by any means. Uh, I follow probably one percent of the tickets, so all the other people who are working on other privacy leaks, like, basically I have to trust they're locking those windows when I'm locking this window over here. And so it's this general principle, we know, like . . . basically what are we all trying to do, we're all following that principle, to fix it everywhere. *It's more of a value than a design thing then, in that respect, maybe.*
> Tor core developer (emphasis added)

That's not to say that innovation on Tor had been lost in favor of minor tweaks and maintenance. From better flow control algorithms to unjam slow patches in the network, to improvements to the core cryptography, to whole new implementations of the basic software and new attack models, Tor continued to be a focal point for innovation, as the largest and most successful practical anonymity network in widespread use. Development began to approach the tricky business of future-proofing the network, with Chelsea Komlo and Isis Lovecruft among the core developers working on protecting Tor against the threats posed by technologies still in their early stages, such as quantum computing.

The engineer world of Tor continued to evolve, not least as more developers joined the project. The vision of privacy in the technical networks of internet power remained, but was progressively incorporating many aspects of the newly value-centered culture in Tor, extending this structural understanding of privacy to the cultures and worlds of the users themselves. The developers increasingly accepted that the ways in which they mapped out privacy might not match those of their users, whose own structures of use

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

and values might not be easily revealed through abstract attack brainstorming and crypto development. Isabela Fernandes, then working as the product manager, began to push internally for a more user-centric approach to design, launching a community team, a substantial program of user research, outreach work in the Global South and East, and devoting substantial development time (and a new user experience team, led by Linda Lee) to improving usability and accessibility for a wider range of users.

The developers not only went to work making Tor slicker and more modern, developing a new look that extended from the browser out to their website, blogs, and training materials, but also developed whole new category systems for understanding and representing their users. Building on this program of user research and outreach, they distilled their experiences into an initial series of *personas* that would act as "ideal" potential users of Tor. This initial set included five personas: Jelani, an LGBTQ activist in Uganda; Fanisa, a person experiencing domestic abuse in Russia; Fernanda, a women's rights activist in Colombia; Fatima, a political researcher in Egypt; and Alex, a journalist in the United States. As can be seen, this is immediately reflective of the kinds of user on which the activist social world in Tor might focus, embodying a vision of Tor that promotes its use for activism, journalism, and social justice and explicitly linking it to other movements and struggles. The documentation around these archetypes describes them as a "vision for who we are designing for [*sic*]." These packaged up and quantified a range of factors, including levels of risk, technological proficiency, their trust of Tor, background, income, connectivity, the languages they speak, the censorship regime in their country, and the devices they use.

Once designed for everyone in the world (and thus, in a sense, for nobody), Tor was now explicitly being designed around a set of particular user archetypes. It was a far cry from the limited behavioral models used in the early 2000s (in which users would visit a certain website multiple times) or the idea of usability from Tor's middle period, as simply becoming more like the rest of the internet. They painted rich pictures of values and use cases, serving as a powerful communication of the values of the project itself. These archetypes have also, since theiy were developed, subtly shaped the development of Tor, giving the engineers a constellation of stars to steer by—real

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

users to imagine, who exist not solely as a set of atomized and contextless behaviors, but who inhabit their own complex cultural worlds.

The engineers' efforts to standardize Tor and incorporate it into other technologies were helped more, paradoxically, by Tor being a value-centered organization than it remaining more ambiguous. Without central coordinating regulators, standards rely on adoption—which itself relies on the project and its vision resonating enough with people to make them want to build things with its tech. Tor's engineers were improving its usability not only for the people downloading the browser, but on the back-end, to make it easier for other developers to plug Tor into their systems, networks, and technologies.[14]

> I think we're going to start seeing a lot more of them as Tor is sort of built into things in ways where you don't even know it's there . . . , I think this is where Tor is heading towards . . . things where Tor is more of a security toolbox, where you can pick and choose which features you want, um, which makes it a lot more applicable to a lot more use cases, um, and I think this is, this is what's needed to get Tor into everything as the . . . the underlying technology for communication.
>
> Tor core developer

This standardization also led Tor's counter-censorship properties to increasingly become a focus of funding and development work of its own. The pluggable transports that initially helped Tor circumvent Chinese censorship developed into the Snowflake project. Although ostensibly a technical engineering solution, Snowflake relied on volunteers to run proxies that would allow users in censored countries to connect to Tor. The Tor Project increasingly tried to make the design and marketing of these appeal to a shared set of values, using drives around real world events (such as protests in Iran in 2022) to present these as easy, effective, and important ways for observers in the West to help.

All this led to major changes in what Tor looked like and how it worked from 2017 onwards. From these engagements with users and the community emerged a much slicker and more modern design—gone were the hackery text on start-up and the old-school interface. Isabela Fernandes would take

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

over the executive director role in 2018, continuing Tor's expansion into new areas of funding, new projects, and new staff in a wide range of roles. Fernandes set about building new alliances in the mode of a professionalized NGO rather than a Wikileaks-style agent of change. The newly transformed Tor Project seemed set for a bright future—assertive, surer of its values, and ready to link up with the new waves of protest and organizing against resurgent authoritarianism around the work. But its rapid expansion, built on the new, less state-reliant funding model, left Tor vulnerable.

In early 2020, just as Tor appeared to be at its zenith, the first wave of lockdowns in response to the COVID-19 pandemic began. In addition to the widespread social disaster, death, and turmoil, this had a catastrophic effect on Tor's new model. Funders suddenly had little money to give, and the general public had even less, meaning that Tor's crowdfunding efforts collapsed. The Electronic Frontier Foundation had spent decades building a strong fundraising profile for itself, but Tor was still in its infancy and was suddenly struggling to survive, having to lay off a number of the new paid developers on staff. There was a broader set of issues underlying this. Despite a number of years of more assertive leadership, Tor was still struggling to articulate its reason for existing to a wider public. Although the Tor Browser was popular, and subsequent releases would adapt it for mobile devices, Tor still lacked a "killer app" that would spark the kind of exponential growth that characterized most internet success stories. But the next steps Tor would take under Fernandes' leadership—as the world emerged from lockdowns and the balance of power in the world began to change dramatically in 2022—were beginning to point the way to a surer future for the project.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

10 PRIVACY FUTURES

Tor had two tough years in 2020 and 2021, as the COVID-19 pandemic swept the world and the organization seemed to have its financial footing cut out from below. Having had to lay off a number of paid developers in a gut-wrenching loss and backtracking on its promising growth in the late 2010s, it looked to many as though Tor's best days—of global relevance and hacker headlines—might be behind it.[1] But, as much of the world opened up again in 2021, so too was Tor able to begin to make up for some of its losses, beginning to grow again and re-establish its finances and alliances. Tor has since begun to regain its footing and its future again looks brighter. Fading into an academic curiosity or a past-its-prime open source foundation now seems far less likely. Although many projects do incredible work away from the limelight, it appears that Tor still has the chance to continue to work at the frontlines of global power and be a key actor in shaping the emerging technopolitics of the near future.

Tor is still searching for what one might have once called its *killer app*—a use case that breaks open a major market or route to mass adoption. It has maintained a solid core of between two and three million daily users around the world for the last decade, but has yet to enter the exponential growth phase that typifies a "success story" in the world of digital infrastructure. Its future funding base is also still an open question—it is still in the early days of building up a solid foundation of donors, and it is heavily reliant on grants from other foundations and companies. At present, Tor is at a crossroads: over the next few years it faces a series of choices about its place in the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

world and will need to square the different visions that still cluster around it. For the final part of this book, I discuss the next chapters in Tor's story: where it might be going, the roles it might play in the future of the internet, and how to make sense of its tangled and complex involvements in digital power.

The same people, groups, ideas, and cultures appear and reappear throughout Tor's life.[2] Although the cultural landscape of the internet infrastructure today looks very different from how it did in the mid-1990s, Tor's three main cultural worlds—the engineers, the maintainers, and the activists—remain rooted in the long-standing traditions and ideas that have shaped the internet. These core worlds and the connections they have to the wider currents of the internet infrastructure will shape what Tor becomes in the future.

One vision of Tor's future—rooted in the engineer's perspective—is for Tor to dissolve into the bloodstream of the internet like a drug, flowing with the other protocols and standards that underpin our digital lives. This would see Tor become more like encryption, simply part of the background hum of the internet without us ever doing anything as clunky as opening up a dedicated Tor Browser. This would entail a wholesale restructuring of the architecture of online power—achieved at the level of the internet's most fundamental protocols.

Some parts of this vision are being realized. Tor is already integrated into Brave browser as a "private browsing mode." Tor waged a long campaign to be formally integrated into Firefox—the browser that the Tor Browser is itself based on—in this way. A subsection of Firefox staff had been trying to convince the foundation to incorporate Tor as a private browsing mode, but this effort ultimately died due to internal rifts within the Firefox project. Although Tor's long-standing efforts to be integrated into Firefox have been abandoned, it has contributed to the browser in a number of other ways. As Tor's developers have hacked on Firefox for years, they have developed wide-ranging security and anti-tracking improvements for it, many of which have been incorporated back into Firefox itself. There is a wealth of space opening up for this tactic of standardization, with Tor (thanks to improvements to the modularization of onion services and its core protocols) now able to be more easily integrated into standalone mobile apps and Internet of Things device standards, and as its security properties (like encryption

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

and authentication) have increasingly become as useful as its privacy and anti-censorship ones (like protecting communications metadata).

But standardization is not the only area in which Tor's technologies are changing. Tor is still far from moving to "maintenance-only mode" and continues in very active technical development. For the engineer world, standardization is a means to spread Tor's structural fix to the landscape of internet power; and as this landscape changes, so too do Tor's technologies in response to new clusters and continents of technological power. As Tor's adversaries reorient themselves in the global threat landscape, there remain important questions about which enemies it will prioritize. And as Tor evolves to meet the shifting tactics of state and corporate surveillance, it is teeing up some tricky design decisions for the future, each in response to a different shift in the technical landscape of power in the internet infrastructure.

One route involves continuing its cat-and-mouse game against the social media and platform giants, through countering their online advertising trackers. These huge companies have laid a mature and extensive surveillance and targeting infrastructure across the world that is not only useful for corporate marketing, but is increasingly used by governments as part of "strategic communications" or "behavior change" campaigns.[3] An active area of continuing development for Tor is in this higher-level design space, above the core protocols that route traffic around the internet, in anti-tracking solutions that allow its users to hide not only from governments, but from platforms as well. And Tor's more foundational functionality is still important in fighting the platforms—even if you remove the trackers, your location is a key part of this targeting ecosystem and when combined with massive corporate databases can be very identifying, and this metadata comes not only from mobile phone location data, but also from your IP address.

Another route would see Tor focus on the spy agencies, beefing up its threat model to include the kinds of global attacks it dismissed in 2002 alongside a range of other nation-state capacities. While Tor protects against some adversaries all of the time, and all adversaries some of the time, it cannot genuinely claim to systematically thwart the full surveillance capacities of the world's most powerful espionage, law enforcement, and military

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

intelligence agencies. These attackers have very extensive (if not global) views of the internet infrastructure and key platforms; very extensive targeting for particular cases, including the ability to compromise target devices directly; and complementary surveillance apparatuses that introduce a wide range of so-called *side channels* that can provide further information to help deanonymize Tor users. One possible model here might see a move from Tor's current low-latency design to include an option to turn on "mid-latency" protections, such as padding, mixing, and delays, that might account for stronger adversaries. This presents a number of issues, not least in reducing the size of the core Tor network, but other security projects are exploring these design options. The past few years have seen a number of competitor projects to Tor emerge, often prioritizing higher security with a trade-off in usability, or focusing on particular applications, such as file sharing, anonymous messaging, or "dead drops" for journalists. However, Tor remains the dominant option. As much as Tor's technical design represents a sweet spot that solves the interests of a range of user groups, it remains true that network effects and cultural alignment—the associations people make with the technology itself—have proven just as important.

Yet another avenue for technical development relates to enabling access to Tor—especially in nations and contexts where it is blocked. This anti-censorship capability positions Tor at the wider front of power between nations—battling not to identify individuals, but to control what their populations see and say, and to influence the public across borders. Many nations have retaliated with sweeping Tor bans, cutting off access to the public: relay operators have faced legal challenges in Russia, and Iran and China (among others) have taken steps to prevent internet service providers from allowing domestic traffic to reach Tor relays. A great deal of the most pressing engineering work related to Tor involves this counter-censorship domain, attempting to build on the clever workarounds that have been developed so far. Projects like Snowflake—in which volunteers serve as proxies to counter censorship by creating new routes to the Tor network—are particularly interesting, combining mass volunteer action with technical design in a way that aligns Tor's engineering with a clear value mission.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Each of these technical design futures are based in the engineer world's visions of rewriting structural power in the internet architecture, but with a slightly different emphasis in each case, focusing on different conflicts, use cases, and domains of privacy. This is less about choosing one path over another, and more about what features the Tor community chooses to emphasize—dictated by personal preferences, but also by funding and changes in wider internet technopolitics. Thus, what happens in Tor's other worlds (both of the people who make it work and of its users) will shape which of these areas develop fastest, as well as which users and use cases, which adversaries and capacities, and which visions of privacy will be most important.

For the maintainers, though increasingly united in a more communal, professionalized culture, the focus remains on the pragmatics of the infrastructure and keeping things running. The relay operators are still at the frontline of state resistance to Tor—the changing strategies that law enforcement use against them will continue to shape the future of the relay community. Although the "neutral" maintainer perspective has become a rather silent one, major changes in the wider landscape of digital technology may well bring it to the fore of the Tor community once again.

Infrastructure is useful on its own, but it becomes particularly powerful in combination with other technologies (in Tor's case, for example, with Bitcoin). If a major, high-throughput killer service—likely either a mass-use messaging app, social media platform, or crypto project—is built on top of Tor and starts to see real adoption, it will begin to face a serious pull to retreat to the "lower layers" as its resources become focused on critical support and maintenance and simply keeping things ticking. As Tor manages to standardize and spread, it might well find major uses in communities with very contrasting politics, which will be hard to square with the strong, value-led mission that has come to predominate within the Tor Project.

One candidate for this movement is becoming increasingly clear. As I write this, different groups of people around the world—in banks, major platforms, start-ups, and online communities—are attempting to imagine new futures of the internet, and to bring these possible realities into being. This is being sold to government policymakers and venture capital firms as

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

the rise of a third era of the internet, following the Web 2.0 of social media with a *Web3* based around decentralized networks of finance, communication, and commerce. This, at least in theory, sees blockchain technologies extended beyond cryptocurrency to provide interoperable shared ledgers for ownership of digital assets, "smart" contracts, portability of content between online communities, and a range of digital ID and assurance functions in the "real" world. These technologies, many of which are fairly old, are based on distributed, cryptographically assured consensus platforms that obviate (again, in theory) the need for a centralized state or governmental body. Although these designs are ideologically libertarian, aiming to undermine the power of states, platforms and financial institutions, they have in fact proven easily co-opted in the interests of capital, and have serious environmental impacts. Despite the money pouring into Web3, it has faced withering criticism and is struggling to reach any mainstream success—it has certainly not been helped by a proliferation of junk currencies, speculative booms, scams, and a wealth of offerings that seem to double down on labor exploitation and social control.

Having largely sat out the dot-com and social media bubbles of venture capital funding, Tor might well be expected to sit out this third great internet hype cycle (with a fourth, artificial intelligence, hot on its heels). In each of these previous booms, the other infrastructures of the internet found their own uses for Tor. But this recent wave has seen more movement in the other direction; Tor has made some serious attempts to engage with cryptocurrencies and other blockchain-based technologies. Due to the ideological alignment between Tor's maintainers and some of the proponents of Web3, including an embrace of decentralization, a history of links with the cryptocurrency space, and a libertarian rather than liberal politics, many within this movement see Tor as a natural ally. There has already been some coordination, as a number of cryptocurrency and decentralized finance projects have begun to encourage their users to donate to Tor, and some in the Tor community have begun to consider the possibilities of incorporating digital currencies into the network itself.

A major development in the technologies of Tor in recent years may make such an alliance more likely. Several core Tor developers have been

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

working on re-implementing Tor in the Rust programming language—a project called Arti. This is funded by ZCash, one of the more cypherpunk cryptocurrencies. In part this is for security reasons: Rust, unlike C, the language in which Tor is currently written, is a far more secure programming language. But this has wider implications. Tor users still mostly access the network through the official Tor Browser, but the Rust implementation (created from scratch) allows for more secure modular use of Tor—embedding it in a crypto wallet, for example. As this use option develops, it will allow crypto projects that survive the coming crashes to build anti-censorship and anonymity properties into their core technical infrastructures and encourage them to install Tor as the supporting infrastructure for whatever they build.

The crypto finance and Web3 communities are not monolithic—they are home to several divergent cultures. Some of these align with Tor's cypherpunk and techno-utopian visions, looking to create censorship-resistant currency and move away from platform-dominant models to a more decentralized economy of digital assets. Others are more interested in novel financial instruments, speculation, or creating artificial scarcity—quite counter to the cypherpunk culture of an internet where ideas can be free and cryptography protects people, rather than profit. Both the engineer ideas of mass-scale disruption or decentralization, as well as a libertarian "neutrality" and distaste for liberal and progressive politics, are features of these wider currents. This has proven an exceptionally difficult balance for Tor to navigate (for many, the libertarian "crypto bro" is a figure of deep derision), but while this ecosystem is awash with billions of dollars in capital, it represents a possible alternative source to crowdfunding and state/NGO money. Whether Tor fully embraces the so-called "crypto revolution," exploits it for financial gain before it collapses into vaporware, or integrates Tor into the few infrastructures that may survive the bubble, Web3 represents, for the moment, a powerful source of money, people, ideology, and culture that Tor will need to reckon with.

If Tor were incorporated into the backbone of the NFT market (or indeed, any other major digital infrastructure), it would pose immediate practical challenges for the Tor network. The additional load and congestion would increase the material and cultural power of the relay operators,

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

as they would become key to scaling up to deal with the new challenges of scale. If it became the foundation of higher-level mass-use infrastructure, Tor's more neutral or neutralized maintainer perspective could be revived; the wide variety of use cases, political diversity, and pragmatic challenges would make overt alignment with political causes far more difficult. In fact, the nascent Web3 has already been an important source of funding for Tor. In 2021, Tor auctioned an NFT, a piece of digital art called *Dreaming at Dusk* created by artist Itzel Yard, based on the private key of the first onion service released on the network.The proceeds from this sale—$1.7 million in the Ethereum cryptocurrency—covered a third of Tor's operating budget for the year, and helped it partly recover following its financial issues faced during the height of the pandemic. This—and other sources of funding—raises broader questions about who has the power to shape Tor's future, and the ways in which Tor's cultures might shape how it evolves.

An alternative future would see Tor take the opposite approach—engaging even more prominently in political battles and embodying the ideas and practices of Tor's relatively newly ascendant activist world. In this vision, Tor would become further connected with social movements and human rights struggles—either internally, through statements of values and organizational practice, or externally, through directly joining coalitions with activist groups and putting Tor's technologies front and center in aligning online privacy with other social justice campaigns. This might see a major liberal philanthropist funding for Tor while it does the hard work of building up a more diversified crowdfunding model.

At the time of writing, Tor's future, dimmed as it struggled through the pandemic and a loss of staff, funding, and direction, has become far clearer. Following the 2022 invasion of Ukraine by Russia, a number of mainstream onion services were created to help Ukrainians and dissident Russians access the wider internet securely. Twitter released its own onion service and the BBC publicized its existing onion service featuring Russian- and Ukrainian-language reporting. As the war progressed, there was evidence of genuinely widespread use of Tor in Ukraine by the public. In the early weeks of the invasion, there were more than 100,000 daily users in Ukraine; in Russia, the invasion saw Tor users drop dramatically, by almost a quarter, after the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

government blocked it, with many switching to bridges and other ways into the network. As the year progressed, other important alignments emerged, with Tor taking a prominent role in connecting protest movements to the wider world in a number of conflicts internationally—not only in Russia's invasion of Ukraine, but also in the rising popular protest movement in Iran and around LGBTQ and abortion rights in the West. Tor's involvement in these struggles appears to be far larger than in the Arab Spring, representing a much wider and more mainstream adoption of its technologies. At the peak of the protests in Iran at the end of the summer in 2022, there were an estimated 500,000 people connecting to Tor there, many via integrated Snowflake proxies. This was a long way from 3,000 people in Cairo, and gives Tor a compelling continuing narrative for why it needs to exist *now*.

These numbers, and the communications from the Tor Project aligning it with these struggles for human rights, can also paint a picture of Tor newly established at the frontlines of Western soft power. Tor can credibly sell itself as the internet for a new Cold War, a framing approach that may not sit well with many members of the internet freedom community. But more liberational and solidarity-oriented futures may well grow from the activist world. Tor's political stances have in the past often been oriented outside the Global West rather than within the United States and Europe, but the rise of authoritarian political movements—particularly in the United States—has led to a reorientation in these places as well. The 2022 US Supreme Court ruling in *Dobbs v. Jackson Women's Health Organization* overturned *Roe v. Wade*, a previous case that enshrined the right to abortion on the grounds of constitutionally protected privacy rights. Following the undoing of those legal rights, many states across the US instituted bans on abortion, with early enforcement already employing online surveillance as the public grew fearful of compelled data sharing by period tracking apps. As US grassroots movements continue to build, this raises the possibility of, rather than elites exporting technologies to support struggles abroad, the people linking up in shared international movements for resistance from below, in which digital privacy activism might be one equal voice among many.

So how might these divergent futures resolve themselves? This book has mapped the stories of three cultures within Tor, born of the foundational

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

cultures of the internet infrastructure and material relationships with the technologies of Tor themselves, which emerged, coexisted, and came into conflict. The tension between these—between privacy as a *structure*, as a *service*, and as a *struggle*—remained stable for much of Tor's life, but as the wider landscape of digital privacy and hacking changed, these contradictions came to a head. The apparent dominance of the activist world in Tor's current era hides complex and still-uneasy alliances.

The new worlds of Tor have their own tensions and faultiness simmering under the surface. There are two main divisions in the new cultural landscape of Tor: one over its relationship to US digital empire, and one over its relationship to crypto. It remains to be seen whether the alliance between the liberal and liberational sides of Tor—between a soft power, top-down, digital development side, and one grounded in a much more radical program of solidarity and struggle from below—remains firm, or whether it will form another cultural split within the community like that between the maintainers and the activists before. This is the new "productively ambiguous" aspect of the detente between cultures in Tor—this time between its radical and liberal currents. Although many of the more politically radical members of Tor have left the project over the last few years, they remain important parts of the wider Tor community (even *in absentia*) and retain a great deal of power to shape what Tor means and how its role in the wider world is perceived. The war in Ukraine and deepening authoritarianism and conflict throughout the world will inflame the contrast between these perspectives—and the role of the United States in these struggles may well prove another fault line within the community.

Similarly, within the engineer and maintainer worlds, the rise of Web3 may provide another rupture, as some of the old cypherpunks remain deep believers in cryptocurrency (as well as cryptography) and a separate crowd hold an instinctive distrust of the NFT space. This Web3 world, rooted in digital cash and financialization, will bring with it questions of Tor's own financial future. It may yet, if it results in boatloads of cash and users, find a new resurgence of a more "neutral" face of Tor, especially if the splits within the activist world become fault lines and fractures.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Tor has successfully walked the fine line on both these issues so far—but this has been enabled by the macroscale cultural and economic environment of the last few years. As this changes, and money, people, and opportunities start to flood in, these splits may well deepen or become full-blown crises. Every source of funding, new alliance, or shift in culture will pull the project in different directions—the future of Tor may be defined by a radically different cultural coalition than that of its past. There is even the possibility of some really odd alliances—for example, a coalition of the more anti-US members of the activist culture and some of the maintainers against those who see Tor through the lens of digital development. And these struggles within Tor aren't limited to the Tor community—they reflect wider conflicts between the cultures of the internet infrastructure and hacker politics.

Despite persistent media accounts of the so-called Dark Web, the worlds of Tor's illicit users and the cryptomarkets remain marginal. One might once have expected this to be a major factor in shaping Tor's future—in 2013, for example, the story was one of struggle between legitimate and illicit use cases, with the cryptomarkets seeming to be a killer app that would grow to dominate other uses of the network. But, as the term Dark Web has expanded to include all online crime, including on social media and messaging apps, crime has become paradoxically less relevant for Tor. Tor has never been usefully incorporated into mass-scale cybercrime infrastructure in any lasting way, and serious organized crime groups—a much more established front of global technopower than the scrappy milieu of small timers operating on cryptomarkets—have never needed to rely on Tor, equipped as they are with botnets, encrypted messaging apps, and illicit VPSes far better suited to their needs.

However, discussions around "online harms" (particularly in the United Kingdom) remain one of the main threats to Tor at the level of domestic policy. Although much of this scrutiny has focused on social media companies, crypto panics are rarely far away. And although crime is unlikely to be the main reason for Tor bans, as we have seen elsewhere, it serves as a useful pretext when a state wishes to ban Tor for other reasons. As authoritarian political movements continue to become established across the word, crime

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

will be cited as a justification to ban Tor in service of state-level power, particularly to undermine its anti-censorship properties.

More extensive critiques of Tor come from commentators like Yasha Levine, whose trawls through emails and financial documents depict Tor as a shadowy organization that colludes with US intelligence services.[4] These largely rely on documents that are publicly hosted on Tor's own website—Tor has never hidden its links with state funding or its historical links with the military, which it shares with almost all foundational computing and communications technologies. There is a deep well of criticism of this side of Tor online, some of which tends toward paranoid conspiracy theory and some which involve a more thoughtful critique of US digital soft power. However, both focus on Tor as something of a monolith—fulfilling a single vision, bound to that of the US government and written into its design and its history.

It's easy to see, with the eye of a journalist, why people may be wary of Tor. It isn't hard to establish a narrative in which Tor is a shadowy tool of US imperialism: it was created by the US Navy, is vulnerable to global adversaries like the NSA, was funded by an ex-CIA front organization, claims to have been pivotal in supporting the Arab Spring, and is now a pillar of the US' communications strategy in Ukraine and Iran. But this perspective misses how contingent each of these developments was—how much of it nearly didn't happen, or almost happened very differently. Tor was only one of dozens of other anonymity networks (and several other onion routing projects) emerging as the Five Eyes global alliance squared off with the Five Ians of the anonymity scene in the late 1990s. Languishing financially in its early years, Tor could have easily died or become another niche open-source software foundation—the IBB funding was by no means an obvious outcome. Similarly, its role in the Arab Spring hinges on accounts that, although part of Tor's own myth-making, are by no means settled. And despite its history often resembling the plot of a spy novel, Tor's historical proximity to espionage and statecraft reflects the ideas and motivations of small numbers of people in a large and diverse community, who have often been much less close to the technical foundations, engineering, or maintenance labor behind Tor than press reporting might make them appear.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

These conspiracist arguments about Tor fundamentally misunderstand what Tor is—it's not a tool, like a Stinger missile that can be smuggled into a country and distributed to particular groups but not others. It's an infrastructure, able to be taken apart, repurposed, and built on by a vast range of different potential users. Tor is compatible both with visions of US soft power, and with more internationalist and solidarity-oriented forms of global struggle against authoritarianism. While the master's tools may not be able to destroy the master's house, the forces of resistance may well be able to drive on—and ultimately seize—the roads laid down by imperial power.

What does all this mean for privacy in the *digital age*? If privacy can be thought of as the practices, technologies, and ideas that we use to demarcate different spaces of power in social life, it's clear that the contemporary internet is the scene of a number of battles over privacy between powerful forces. These include the deepening conflicts between the US, China, and Russia; the rise of a dispersed global authoritarian fascist movement; the growth of an aligned technological and financial system that places power in the hands of small numbers of extremely powerful companies (both platforms and financial institutions) implicated in new forms of digital colonialism; and, finally, state attempts to govern their own populations in an era of panics about online harm. While many of these conflicts are squarely in the material domain—who controls the physical landscape of control points that give different actors power over the internet and digital society—they also spill into the domain of culture: how these are used to communicate and fight for ideas, values, and competing visions of the future.

The common thread between these, which brings Tor to the frontline of these battles, is the role played by infrastructure—crucially, the ability of communications infrastructures to embed power and control at the level of its most basic protocols, often relying at its base on the ability to identify individuals and the traces they leave. While Tor doesn't destroy digital power entirely, it does design out many of these control points in the lower layers, moving contests over control up the stack into places where people who aren't engineers or technocrats can have a say. It takes these radically new and deep forms of power over communication and hands them to the users. Although this tries to undo much of the dystopian progress of the last twenty

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

years, it does not represent a return to a pre-internet distribution of power. Instead, it hearkens back to the utopian vision of the internet expressed in the early hacker manifestos, which, free from its own built-in control points, could break down the barriers between traditional systems of control both intimate and global. This vision is not without its flaws—where America and the broader West have attempted to impose idealistic "flat" structures for communication and commerce from above, this has rarely ended well.

It is hardly surprising that the interests of American global power might occasionally and in limited ways align with those of techno-libertarian hackers, anarchist cryptographers, groups resisting authoritarian states, and lawyer-activists seeking to backstop liberal, democratic values. These kinds of uneasy coalitions between power and resistance have defined every communications infrastructure throughout history, and these are the cultures that have swirled around the technologies of the internet for much of its life. Although this infrastructure's design and material shape undoubtedly crystallize the politics of its early designers—a mix of the US' 1990s military-academics and the libertarian visions of the cypherpunks—the history of the internet is defined above all by the efforts that hackers, engineers, and everyday users have made to take the apparently fixed properties of its infrastructures and break them, or to build new and diverse worlds out of them.

This is all to say that, rather than a rote rehearsal of the values designed into Tor's code, the actual ways in which it has acted in the world and will act in the future, and the effects it has had on the landscape of digital power (in the intimate spaces of people's lives and the wider vistas of technopolitics on the global scale), are all contingent on the different people, cultures, and ideas that have clustered around it. Who has used it, who has joined its communities, who maintains it, who has built on it and built practices around it, who has funded and fought for it, and who has attacked it, undermined it, or banned it—these people have shaped what Tor is and does, and in many cases they have protected its technologies as much as they have been protected *by* them. Tor's present was not predestined in the code, but was accomplished by people (both hidden and visible) doing myriad different kinds of work. Its future is not set, but it is something that will be struggled over.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

The biography of Tor is the story of a profound *hack* at the heart of the internet—a wildly successful attempt to change the basic laws of physics written into its fundamental protocols. But, as the engineers found, it's not as simple as backstopping this all with crypto and a clever design—sealing the blueprint for a new society into the math. Ultimately, the question became about not only what power relationships are built into the tech, but the ability of different groups—users, activists, journalists, spies, policymakers, and different factions with the Tor Project itself—to build different meanings, and forms of privacy, around the tech. So the ultimate *meaning* of Tor—whether it is the kind of privacy imagined by the US State Department, or by a group of Tunisian activists, or a person in their bedroom—is an achievement, not a given. It is the result of many different people pulling at the same time, and not always in the same direction.

I wrote a large part of this book across a four-day conference in Lausanne, Switzerland in early 2022. It was the first conference I had attended in person after two years of tele-presentations during the COVID-19 pandemic. Although my more sensible colleagues flew to Lausanne from Edinburgh, I took an ill-advised 14-hour train journey each way, traveling along the stunning Scottish Southeastern coastline, through an England convulsed by political aftershocks of Brexit and COVID-19, under the gray waters of the English Channel and tracing the undersea cables connecting the United Kingdom to Europe's internet, sprinting across Paris to make a final three-hop connection of my own, finally rolling through the Swiss fog and up through the Alps. On the return leg, as Russian shelling intensified in Kyiv, I thought to check the Tor Metrics site to see whether Tor had seen a spike in users in Russia or Ukraine.

Instead of the logo of the now-defunct Virgin Rail that I had seen six years earlier, the somewhat less shiny block page of the London North Eastern Railway company (the state provider who had taken over from Virgin) proclaimed:

> LNER
> This site is blocked due to content filtering:
> metrics.torproject.org

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

> Site blocked. metrics.torproject.org is not allowed on this network for the protection of all service users. This site was blocked due to the following categories: **Proxy/Anonymizer**
> If you feel this domain has been incorrectly blocked please contact redacted@lner.co.uk stating your date and time of travel and which domain/site you have been prevented from accessing.
> Thank you
> IT Support
> London North Western Railway

Noting that the IT support staff had managed to get the name of their own company wrong, I picked up my mobile phone, opened the Tor Browser app (far sleeker than the browser I had used back in 2016), and watched the page load.

Tor isn't a parasite on the internet—it is part of the internet. The cultures that surround and shape it are extensions of the very cultures that have grown up around the internet infrastructure since its earliest beginnings in the 1960s. Nothing could be more quintessentially of the internet than Tor—by turns scrappy and professional, a frontline of both international resistance and of US power, a battleground between spies and woven through everyday lives, depicted as a haven of crime and a space for revolutionary new ways of living. The people who have made it a reality—from all parts of the Tor community throughout the years—are building one possible future of what used to be called the *internet galaxy*. The cluster of strange worlds orbiting around Tor by and large don't see themselves as strands of a Dark Web, but rather as something closer to an Eternity Service: the infrastructure of a brighter internet.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

AFTERWORD

Although I have left social theory very much in the background throughout this book, my approach is shaped by ideas from Science and Technology Studies (STS) scholars—particularly Robin Williams and Neil Pollack's developments of approaches to studying technologies through "biographies of artifacts and practices" and Susan Leigh Star and Geoffrey Bowker's "social worlds" scholarship. Both of these prioritize *long durée* cultural and historical studies across multiple sites, and both contributed to this book. I am also particularly indebted to the scholarship of Gabriella Coleman, Stefania Milan, Sarah Myers West, Helen Nissenbaum, Francesca Musiani, and Laura DeNardis, whose work underpins many of the ideas in this book. My approach to these frameworks has also been strongly shaped by Stuart Hall's cultural studies scholarship. I also want to highlight two scholars whose PhDs on Tor were contemporaneous with my own—Nathalie Marechal and Daniele Pizio—with Nathalie focusing on Tor's role in social movements for digital rights, and Daniele conducting a parallel STS study of Tor.[12]

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Notes

CHAPTER 1

1. Seda Gürses, Arun Kundnani, and Joris Van Hoboken, "Crypto and Empire: The Contradictions of Counter-surveillance Advocacy," *Media, Culture & Society* 38, no. 4 (2016): 576–590.
2. For example, Solove identifies more than 40 distinct kinds of "privacy" violation solely in terms of US law in Solove, "A Taxonomy of Privacy."
3. Chris Hall, Ross Anderson, Richard Clayton, Evangelos Ouzounis, and Panagiotis Trimintzios, "Resilience of the Internet Interconnection Ecosystem," in *Economics of Information Security and Privacy III*, 119–148 (New York: Springer, 2013).
4. Rajkumar Buyya, Mukaddim Pathan, and Athena Vakali, eds., *Content Delivery Networks*, vol. 9 (Berlin: Springer Science & Business Media, 2008).
5. M. Cayford, C. Van Gulijk, and P. H. A. J. M. van Gelder, "All Swept Up: An Initial Classification of NSA Surveillance Technology," in *Safety and Reliability: Methodology and Applications*, 643–650 (Boca Raton, FL: CRC Press, 2014).
6. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine, "Browser Fingerprinting: A Survey," *ACM Transactions on the Web (TWEB)* 14, no. 2 (2020): 1–33.
7. Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
8. Ben Collier, Gemma Flynn, James Stewart, and Daniel Thomas, "Influence Government: Exploring Practices, Ethics, and Power in the Use of Targeted Advertising by the UK State," *Big Data & Society* 9, no. 1 (2022).
9. Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet." *Survival* 58, no. 1 (2016): 7–38.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

10. Julie E. Cohen, "What Privacy Is For," *Harvard Law Review* 126, no. 7 (2013): 1904–1933.

11. As set out in the influential *Harvard Law Review* paper "The Right to Privacy" by Warren and Brandeis, itself a response to technological changes in the media of the late 1800s.

12. Norbert Elias, *The Civilizing Process* (Oxford: Blackwell, 1969).

13. Yuanye Ma, "Relational Privacy: Where the East and the West Could Meet," *Proceedings of the Association for Information Science and Technology* 56, no. 1 (2019): 196–205.

14. I. Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?" *Journal of Social Issues* 33, no. 3 (1977): 66–84; A. Moore, "Privacy: Its Meaning and Value," *American Philosophical Quarterly* 40, no. 3 (2003): 215–227.

15. Christina B. Whitman, "Privacy in Confucian and Taoist Thought," in *Individualism and Holism: Studies in Confucian and Taoist Values*, ed. by D. Munro (Ann Arbor: University of Michigan Center for Chinese Studies, 1985).

16. Susan S. M. Edwards, *Policing "Domestic" Violence: Women, the Law and the State* (Thousand Oaks, CA: Sage Publications, 1989).

17. Helen Nissenbaum, "Privacy in Context," in *Privacy in Context* (Palo Alto, CA: Stanford University Press, 2009).

18. Lawrence Lessig, "The Architecture of Privacy," *Vanderbilt Journal of Entertainment and Technology Law* 1, no. 1 (1999): 56.

19. Madeleine Akrich, Wiebe E. Bijker, and John Law, *Shaping Technology/Building Society: Studies in Sociotechnical Change* (Cambridge, MA: MIT Press, 1992), 205.

20. Manuel Castells, *The Network Society* (London: Edward Elgar, 2004).

21. Laura DeNardis and Francesca Musiani, "Governance by Infrastructure," in *The Turn to Infrastructure in Internet Governance*, ed. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 3–21 (New York: Palgrave Macmillan, 2015).

22. DeNardis and Musiani, "Governance by Infrastructure."

23. As of the time of writing; when this goes to print, the number may be substantially lower.

24. Adele E. Clarke and Susan Leigh Star, "The Social Worlds Framework: A Theory/Methods Package," in *The Handbook of Science and Technology Studies* 3, no. 0 (2008): 113–137.

25. J. C. York, *Silicon Values: The Future of Free Speech under Surveillance Capitalism* (New York: Verso Books, 2022).

26. More radical visions of crypto-privacy can be found in Britt S. Paris, Corinne Cath, and Sarah Myers West, "Radical Infrastructure: Building Beyond the Failures of Past Imaginaries for Networked Communication," *new media & society*, first published online February 3, 2023, https://doi.org/10.1177/14614448231152546.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

CHAPTER 2

1. Roy Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet," *The American Historical Review* 103, no. 5 (December 1998): 1530–1552.
2. Roy Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet," *American Historical Review* 103, no. 5 (1998): 1530–1552.
3. Raphael Cohen-Almagor, "Internet History." In *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (IGI Global, 2013), 19–39; James Curran, "Rethinking internet history: James Curran." In *Misunderstanding the Internet* (Routledge, 2012), 40–71; Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (October 2009): 22–31.
4. Richard Kerbaj, *The Secret History of the Five Eyes: The Untold Story of the International Spy Network* (London, Bonnier, 2023).
5. Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Camrbidge: MIT Press, 1997).
6. Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers."
7. Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers."
8. Steven Levy, *Hackers: Heroes of the Computer Revolution* (New York: Anchor Press/Doubleday, 1984); Brent Jesiek, "Democratizing software: Open source, the hacker ethic, and beyond," *First Monday* 8, no. 10 (October 2003).
9. Majid Yar, "Virtual Utopias and Dystopias: The Cultural Imaginary of the Internet." In *Utopia: Social Theory and the Future* , ed. Keith Tester and Michael Hviid Jacobsen (London: Routledge, 2012), 179–195.
10. E. Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton: Princeton University Press, 2013); Kevin F. Steinmetz, *Hacked: A Radical Approach to Hacker Culture and Crime* (New York: New York University Press, 2016); Stefania Milan and Lonneke van der Velden, "The Alternative Epistemologies of Data Activism," *Digital Culture & Society* 2, no. 2 (2016): 57–74.
11. E. Gabriella Coleman and Alex Golub, "Hacker practice: Moral genres and the cultural articulation of liberalism," *Anthropological Theory* 8, no. 3 (2008): 255–277.
12. Coleman and Golub, "Hacker practice."
13. For a more recent exploration of cypherpunks and other crypto-activists, and a rich theoretical discussion of the political importance of the design of crypto systems, see S. M. West, "Survival of the Cryptic: Tracing Technological Imaginaries across Ideologies, Infrastructures, and Community Practices," *New Media & Society* 24, no. 8 (2022): 1891–1911, https://doi.org/10.1177/1461444820983017.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

14. Eric Hughes, "A Cypherpunk's Manifest," http://www.activism.net/cypherpunk/manifesto.html. An archived copy of the cypherpunks mailing list can be downloaded at: http://mailing-list-archive.cryptoanarchy.wiki.

15. Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (New York: Penguin, 2002). Tim Jordan and Paul Taylor, "A sociology of hackers," *The Sociological Review* 46, no. 4 (November 1998): 757–780.

16. Coleman, *Coding Freedom*.

17. David M. Berry, *Copy, Rip, Burn. The Politics of Copyleft and Open Source* (London: Pluto Press, 2008); Allison Powell, "Democratizing production through open source knowledge: from open software to open hardware," *Media, Culture & Society* 34, no. 6 (August 2012): 691–708.

18. Reid Skibell, "The Myth of the Computer Hacker," *Information, Communication & Society* 5, no. 3 (2002): 336–356; Bruce Sterling, *The Hacker Crackdown* (New York: Bantam, 1993).

19. Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers," 1544.

20. Coleman and Golub, "Hacker practice."

21. Michael Bachmann, "Deciphering the Hacker Underground: First Quantitative Insights." In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (IGI Global, 2012), 175–194.

22. Paul Taylor, *Hackers: Crime and the Digital Sublime* (Routledge, 1999).

23. J. M. Chenou, "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s," *Globalizations* 11, no. 2 (2014): 205–223.

24. Sangmoon Kim, "The diffusion of the Internet: Trend and causes," *Social Science Research* 44, no. 2 (March 2011): 602–613.

25. Loïc Wacquant, "Three Steps to a Historical Anthropology of Actually Existing Neoliberalism," *Social Anthropology* 20, no. 1 (February 2012): 66–79.

26. Wacquant, "Three Steps."

27. Adam Crawford, "Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security," *Theoretical Criminology* 10, no. 4 (November 2006): 449–479.

28. Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992).

29. Jochen Von Bernstorff, "Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony," *European Law Journal* 9, no. 4 (September 2003): 511–526; Jean-Marie Chenou, "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s," *Globalizations* 11, no. 2 (February 2014): 205–223.

30. John Lanchester, "Document Number Nine," review of *The Great Firewall of China*, by James Griffiths and *We Have Been Harmonised*, by Kit Strittmatter, *London Review of Books*, October 10, 2019.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

31. Jean-Marie Chenou, "From cyber-libertarianism to neoliberalism"; Victor Pickard, "Neoliberal Visions and Revisions in Global Communications Policy from NWICO to WSIS," *Journal of Communication Inquiry* 31, no. 2 (2007): 118–139.

32. Graham Thomas and Sally Wyatt, "Shaping cyberspace—interpreting and transforming the Internet," *Research Policy* 28, no. 7 (September 1999): 681–698.

33. Laura DeNardis, "A history of internet security." In *The History of Information Security: A Comprehensive Handbook*, ed. by Karl De Leeuw and Jan Bergstra (Elsevier Science, 2007): 681–704.

34. Linda Monsees, *Crypto-Politics: Encryption and Democratic Practices in the Digital Era* (Routledge, 2019).

35. DeNardis, "A history of internet security."

36. Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science and Technology Law Review* 13 (2012).

37. DeNardis, "A history of internet security."

38. Steven Levy, "Crypto rebels," in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* ed. by Peter Ludlow (Cambridge: MIT Press, 1996): 185–205.

39. Tobias Burgers and David Ryland Scott Robinson, "Keep Dreaming: Cyber Arms Control is Not a Viable Policy," *Sicherheit und Frieden (S+ F)/Security and Peace* 36, no. 3 (2018): 140–145.

CHAPTER 3

1. Christof Demont-Heinrich, "Central Points of Control and Surveillance on a 'decentralized' Net: Internet service providers, and privacy and freedom of speech online," *info* 4, no. 4 (2002): 32–42.

2. Graham Thomas and Sally Wyatt, "Shaping cyberspace—Interpreting and transforming the Internet," *Research Policy* 28, no. 7 (September 1999): 681–698.

3. Matthew Edman and Bülent Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," *ACM Computing Surveys* 42, no. 1 (December 2009): 1–35.

4. David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. "Hiding Routing Information." In *Information Hiding: First International Workshop Cambridge, UK, May 30–June 1, 1996 Proceedings* (Berlin: Springer Berlin, Heidelberg, 2005), 137–150.

5. David L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM* 24, no. 2 (February 1981) 84–90.

6. David M. Goldschlag, Michael Reed, and Paul Syverson, "Onion routing," *Communications of the ACM* 42, no. 2 (February1999): 39–41.

7. Goldschlag, Reed, and Syverson, "Hiding Routing Information."

8. A discussion of the Onion Dinner can be found in the *NRL onions@ list archives* at https://www.onion-router.net/Archives/onions-1997.txt.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

9. A much richer history of the cypherpunks and contrasting visions of cryptography (and their problems) can be found in Sarah Myer West's scholarship, notably Sarah Myers West, "Survival of the cryptic: Tracing technological imaginaries across ideologies, infrastructures, and community practices," *New Media & Society* 24, no. 8 (August 2022): 1891–1911 and Sarah Myers West, "Cryptographic imaginaries and the networked public." *Internet Policy Review* 7, no. 2 (May 2018).

10. This phrase was originally used by Lorrie Cranor (now a professor at Carnegie Mellon University) to describe the Crowds anonymity system. See also Roger Dingledine and Nick Mathewson, "Anonymity Loves Company: Usability and the Network Effect." In Proceedings of the Fifth Workshop on the Economics of Information Security (2006).

CHAPTER 4

1. Matthew Crain, "Financial markets and online advertising: Reevaluating the dotcom investment bubble," *Information, Communication & Society* 17, no. 3 (January 2014): 371–384.

2. David Lyon, *Surveillance after Snowden* (Cambridge: Polity, 2015).

3. Markus Giesler and Mali Pohlmann, "The Anthropology of File Sharing: Consuming Napster as a Gift," *Advances in Consumer* 30, no. 1 (2003), 273–279.

4. Ross Anderson, "The Eternity Service." In *Proceedings of PRAGOCRYPT*, vol. 96 (1996), 242–252.

5. The visions of electronic payment systems and digital currency underpinning the Eternity Service would later also influence the development of cryptocurrencies like Bitcoin.

6. Raphaël Nowak and Andrew Whelan, "Editorial: On the 15-year anniversary of Napster-Digital music as boundary object," *First Monday* (2014).

7. A more extended list of these can be found in the initial Tor design publication. See R. Dingledine, N. Mathewson, and P. F. Syverson, "Tor: The Second-Generation Onion Router," in *USENIX Security Symposium* 4 (2004): 303–320.

8. Roger Dingledine, "The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven" (master's thesis, Massachusetts Institute of Technology, 2000).

9. George Danezis, Roger Dingledine, and Nick Mathewson, "Mixminion: Design of a type III anonymous remailer protocol," In *2003 Symposium on Security and Privacy, 2003*, (IEEE Computer Society, May 2003), 2–15.

10. Dingledine, "Free Haven Project."

11. Tor was the third generation of the onion routing design—its main core difference from the NRL's first and second generation systems was in the design of the "onion" of encrypted metadata layers. Tor adding a "telescoping" onion design that allowed forward secrecy in the circuit. For more detail on the evolution between these versions, see Paul Syverson, "A Peel of Onion" (Twenty-Seventh Annual Computer Security Applications Conference, Orlando, Florida, December 2011).

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

12. David Cole, "We Kill People Based on Metadata," *The New York Review of Books*, May 10, 2014.

13. See e.g. Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Wiley, 2020).

14. David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique," *Big Data & Society* 1, no. 2 (July 2014).

15. Claudia Diaz, Stefaan Seys, Joris Claessens, and Bart Preneel, "Towards Measuring Anonymity." In *Proceedings of Privacy Enhancing Technologies Workshop* ed. Roger Dingledine and Paul Syverson (April 2002); Andrei Serjantov and George Danezis, "Towards an Information Theoretic Metric for Anonymity." In *Proceedings of Privacy Enhancing Technologies Workshop*, ed. Roger Dingledine and Paul Syverson (April 2002).

16. Paul Syverson, "Why I'm Not an Entropist." In *Security Protocols XVII: 17th International Workshop, Cambridge, UK, April 1–3, 2009. Revised Selected Papers 17*, ed. Bruce Christianson, James A. Malcolm, and Vashek Matyás (Springer, 2013).

17. Syverson, "Why I'm Not an Entropist."

18. Later developed in the "20,000 in League Under the Sea" paper, which allows for these concentrations in the network to be mapped over probability distributions. See A. D. Jaggard, A. Johnson, S. Cortes, P. Syverson, and J. Feigenbaum, "20,000 in League Under the Sea: Anonymous Communication, Trust, MLATs, and Undersea Cables," *Proceedings on Privacy Enhancing Technologies* 2015, no. 1 (2015): 4–24.

19. This is very similar to Musiani and De Nardis' descriptions of "control points" in the internet infrastructure.

20. Catherine Meadows at the Naval Research Laboratory made some particularly important contributions to these early design stages.

21. Joan Feigenbaum, Aaron Johnson, and Paul Syverson, "A model of onion routing with provable anonymity." In *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12–16, 2007. Revised Selected Papers 11* (Springer 2007), 57–71.

CHAPTER 5

1. Susan Leigh Star, Susan Leigh, "The Ethnography of Infrastructure," *American Behavioral Scientist* 43, no. 3 (November 1999): 377–391.

2. "Relay Operation," Tor Project, https://community.torproject.org.

3. Rob Jansen, Kevin S. Bauer, Nicholas Hopper, and Roger Dingledine, "Methodically Modeling the Tor Network," *CSET '12, 5th Workshop on Cybersecurity Experimentation and Test* (August 2012).

4. Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," *Proceedings of the 13th USENIX Security Symposium* (August 2004).

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

5. E. Gabriella Coleman and Alex Golub, "Hacker practice: Moral genres and the cultural articulation of liberalism," *Anthropological Theory* 8, no. 3 (2008): 255–277.
6. Gabriella Coleman, "The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld," *Anthropological Quarterly* 83, no.1 (Winter 2010): 47–72.
7. Sebastiaan Gorissen and Robert W. Gehl, "When Wikipedia met Tor: trials of legitimacy at a key moment in internet history," *Internet Histories* 7, no. 2 (December 2021): 1–17.
8. Gorissen and Gehl, "When Wikipedia met Tor."
9. Dingledine, Mathewson, and Syverson, "Tor," 115.
10. Dingledine, Mathewson, and Syverson, "Tor."
11. Camille Akmut, "Lustrum, the oldest relays of the Tor network and their ISP's: more data," *Privacy Enhancing Technologies* (June 2019).
12. Camille Akmut, "Fearless, 1000 days and still running: the 'most resilient' exit nodes of the Tor network and their ISP'–a quantitative approach," *Privacy Enhancing Technologies* (2019).
13. E. Gabriella Coleman, "The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast," *Anthropological Quarterly* 77, no. 3 (Summer 2004): 512.
14. Dawn Nafus, "'Patches don't have gender': What is not open in open source software," *New Media & Society* 14, no. 4 (2011): 669–683.

CHAPTER 6

1. Steven M. Furnell, Paul S. Dowland, and Peter W. Sanders, "Dissecting the "Hacker manifesto," *Information Management & Computer Security* 7, no. 2 (May 1999): 69–75.
2. Bruce Sterling, *The Hacker Crackdown* (New York: Bantam, 1993).
3. Sterling, "The Hacker Crackdown."
4. Mitchell Kapor and John Perry Barlow, "Across the Electronic Frontier," *Electronic Frontier Foundation*, July 10, 1990.
5. Hector Postigo, *The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright* (Cambridge: MIT Press, 2012).
6. George R. Urban, *Radio Free Europe and the Pursuit of Democracy: My war Within the Cold War* (New Haven: Yale University Press, 1997).
7. Monroe Price, "Public Diplomacy and the Transformation of International Broadcasting," *Cardozo Arts and Entertainment Law Journal* 21, no. 1 (2003): 51–85.
8. Emily T. Metzgar, "Considering the 'Illogical Patchwork': The Broadcasting Board of Governors & US International Broadcasting," *CPD Perspectives: University of Southern California Center on Public Diplomacy* (February 2013).
9. "Reports," Tor Project, https://www.torproject.org/about/reports/.
10. Charlie Beckett and James Ball, *WikiLeaks: News in the networked era* (Cambridge: Polity, 2012).

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

11. Raffi Khatchadourian, "No Secrets," *The New Yorker*, June 7, 2010.
12. Kim Zetter, "WikiLeaks Was Launched With Documents Intercepted From Tor," *Wired*, June 1, 2010.
13. David Leigh, "US embassy cables leak sparks global diplomatic crisis," *The Guardian*, November 28, 2010.
14. Chris Kelty, *Two Bits: The Cultural Significance of Free Software* (Durham: Duke University Press, 2008).
15. Matt Goerzen and Gabriella Coleman, "Wearing Many Hats," *Data and Society* (2022).
16. Bryan Pfaffenberger, "The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing," *Knowledge, Technology & Policy* 13, no. 3 (2000): 78–92.
17. Andrew O'Hagan, "Ghosting," *London Review of Books* March 6, 2014.
18. For a wider discussion of bike-shedding, see Poul-Henning Kamp's email at https://bikeshed.com for its infamous application of Parkinson's law in a hacker context.
19. Jaap-Henk Hoepman and Bart Jacobs, "Increased security through open source," *Communications of the ACM* 50, no.1 (2007): 79–83.
20. Mike Perry, Erinn Clark, Steven Murdoch, and Georg Koppen, "The design and implementation of the Tor Browser," *Technical Report* (2018).

CHAPTER 7

1. Karsten Loesing, Steven Murdoch, and Roger Dingledine, "A Case Study on Measuring Statistical Data in the Tor Anonymity Network." In *Financial Cryptography and Data Security, FC 2010 Workshops, RLCPS, WECSR, and WLC2010, Tenerife, Canary Islands, Spain, January 2010, Revised Selected Papers* (Springer 2010): 203–215.
2. Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (Brooklyn, Melville House, 2015).
3. Gabriel Weimann, "Going Dark: Terrorism on the Dark Web," *Studies in Conflict & Terrorism* 39, no. 3 (2016): 195–206.
4. In fact, it was originally coined by Michael Bergman to illustrate the difficulties early web search engines had indexing useful data stored in public online archives, a context in which it makes much more sense than in the discussing of crime and online security.
5. A related point regarding the overwhelming focus on tiny numbers of technically sophisticated hacks over wide scale "abuse" was made by Alex Stamos in his keynote address, "Tackling the Trust and Safety Crisis," at the 28th USENIX Security Conference Symposium in 2019.
6. Robert W. Gehl, "Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network," *New Media & Society* 18, no. 7 (August 2016): 1219–1235; Michael Chertoff, "A public policy perspective of the Dark Web," *Journal of Cyber Policy* 2, no. 1 (March 2017): 26–38.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

7. David S. Wall and Matthew L. Williams, "Policing cybercrime: networked and social media technologies and the challenges for policing," *Policing and Society* 23, no. 4 (March 2013): 409–412.
8. Alice Hutchings and Thomas J. Holt, "The online stolen data market: disruption and intervention approaches," *Global Crime* 18, no. 1 (2017): 11–30.
9. "How Onion Services Work," Tor Project, https://community.torproject.org/onion-services/overview/.
10. This functions a bit like Anderson's Eternity Service or Dingledine's Free Haven except that it hosts the directory rather than the files themselves.
11. David Lee Chaum, "Computer systems established maintained and trusted by mutually suspicious groups," PhD diss. (University of California, Berkeley, 1982).
12. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008).
13. Cryptocurrencies, despite popular belief, do not on their own offer any meaningful anonymity protections.
14. Stefan Scharnowski and Yanghua Shi, "Bitcoin blackout: Proof-of-work and the centralization of mining," (November 2022).
15. Chelsea Manning, *Readme.txt* (New York: Farrar, Straus and Giroux, 2022).
16. Roger Huang, "How Bitcoin and Wikileaks Saved Each Other," *Forbes*, April 26, 2019.
17. Joe Mullin, "'I have secrets: Ross Ulbricht's private journal shows the Silk Road's birth," *Ars Technica*, January 21, 2015.
18. Judith Aldridge and David Décary-Hétu. "Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation," (May 2014).
19. Aldridge and Décary-Hétu, "Not an 'Ebay for Drugs.'"
20. Alexia Maddox, Monica J. Barratt, Matthew Allen, and Simon Lenton, "Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde,'" *Information, Communication & Society* 19, no. 1 (October 2015): 111–126.
21. Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable," *Gawker*, June 1, 2011.
22. Mullin, "I have secrets."
23. Isak Ladegaard, "We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets," *The British Journal of Criminology* 58, no. 2 (March 2018): 414–433.
24. Monica J. Barratt, Simon Lenton, Alexia Maddox, and Matthew Allen, "'What if you live on top of a bakery and you like cakes?'—Drug use and harm trajectories before, during and after the emergence of Silk Road," *International Journal of Drug Policy* 35 (April 2016): 50–57.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

25. David Décary-Hétu and Luca Giommoni, "Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous," *Crime, Law and Social Change* 67, no. 1 (February 2017): 55–75.

26. Patrick Howell O'Neill, "The Police Campaign to Scare Everyone Off of Tor," *Daily Dot*, November 7, 2014.

27. The OnionScan project is available at https://onionscan.net.

28. Isak Ladegaard, ""I Pray That We Will Find a Way to Carry on This Dream": How a Law Enforcement Crackdown United an Online Community," *Critical Sociology* 45, no. 4–5 (July 2019): 631–646.

29. Ladegaard, "'I Pray That We Will Find a Way to Carry on This Dream.'"

30. Angus Bancroft and Peter Scott Reid, "Challenging the techno-politics of anonymity: the case of cryptomarket users," *Information, Communication & Society* 20, no. 4 (2017): 497–512.

31. Kimberley Masson and Angus Bancroft, "'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets," *International Journal of Drug Policy* 58 (August 2018): 78–84.

32. Martin Horton-Eddison, Patrick Shortis, Judith Aldridge, and Fernando Caudevilla, "Drug Cryptomarkets in the 2020s: Policy, Enforcement, Harm, and Resilience," *Swansea: Global Drug Policy Observatory* (June 2021).

33. Monica J. Barratt and Judith Aldridge, "Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask)," *International Journal of Drug Policy* 35 (September 2016): 1–6.

34. Stefania Milan, "Data activism as the new frontier of media activism." In *Media Activism in the Digital Age*, ed. Goubin Yang and Viktor Pickard (New York: Routledge, 2017).

35. Ben Collier and Richard Clayton, "A 'sophisticated attack'? Innovation, technical sophistication, and creativity in the cybercrime ecosystem," Paper presented at *Workshop on the Economics of Information Security, Tulsa, Oklahoma, June 21–22, 2022*.

36. Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime* (Cambridge: Harvard University Press, 2018).

37. Matteo Casenove and Armando Miraglia, "Botnet Over Tor: The Illusion of Hiding." In *2014 6th International Conference On Cyber Conflict (CyCon 2014), June 3–6, Tallinn, Estonia, 273–282* (Tallin: NATO CCD COE Publications).

38. Gemma Davies, "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers," *The Journal of Criminal Law* 84, no. 5 (October 2020): 407–426.

39. "No Hiding Place for Online Criminals," GCHQ, https://www.gchq.gov.uk/news/gchq-and-nca-join-forces-ensure-no-hiding-place-online-criminals.

40. This continued until the late 2010s, and in 2018, Torservers was raided by German police.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

41. Eva Galperin, "Access Now and EFF Condemn the Arrest of Tor Node Operator Dmitry Bogatov in Russia," *Electronic Frontier Foundation*, April 24, 2017.

42. Tor is in fact a very useful investigation tool for law enforcement, private detectives, and those fighting child abuse online, as it allows them to access harmful websites without revealing to the people who run them that they are police.

CHAPTER 8

1. Arnold S. De Beer, "The internet in Africa—A new road to developmental opportunities or a digital highway leading to nowhere?" *South-North Cultural and Media Studies* 15, no. 1–2 (2001): 135–153.

2. Joseph Nye Jr, "The information revolution and American soft power," *Asia Pacific Review* 9, no. 1 (2002): 60–76.

3. Michael Kwet, "Digital colonialism: US empire and the new imperialism in the Global South," *Institute of Race Relations* 60, no. 4 (April–June 2019): 3–26.

4. William Lafi Youmans and Jillian C. York, "Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements," *Journal of Communication* 62, no. 2 (April 2012): 315–329.

5. Rohan Grover, "The geopolitics of digital rights activism: Evaluating civil society's role in the promises of multistakeholder internet governance," *Telecommunications Policy* 46, no. 10 (November 2022).

6. Nathaniel Rich, "The American Wikileaks Hacker," *Rolling Stone*, December 1, 2010.

7. Jillian York, "Jacob Appelbaum presents Tor at Arab Bloggers Workshop 2009," *Global Voices Advox*, December 9, 2009.

8. As shown in, e.g., https://www.youtube.com/watch?v=bIvt9snFQig, a session from a Cairo-based IT conference called Cairo ICT in 2011, featured in Laura Poitras's film *Risk*.

9. Shoshana Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization," *Journal of information technology* 30, no. 1 (2015): 75–89; Sarah Myers West, "Data capitalism: Redefining the logics of surveillance and privacy," *Business & society* 58, no. 1 (2019): 20–41.

10. Rama Halaseh, "Civil society, youth and the Arab Spring." *In Change and Opportunities in the Emerging Mediterranean*, ed. Stephen Calleya and Monika Wohlfeld (Malta: University of Malta, 2012), 254–273.

11. Habibul Haque Khondker, "Role of the new media in the Arab Spring," *Globalizations* 8, no. 5 (2011): 675–679.

12. Amy E. Cattle, "Digital Tahrir Square: An Analysis of Human Rights and the Internet Examined Through the Lens of the Egyptian Arab Spring," *Duke Journal of Comparative & International Law* 26 (2015): 417–449.

13. Though these are, given the anonymous nature of Tor, somewhat unreliable. What they do provide evidence for is an increase in Tor use (from a low baseline) around the time of the

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

protests and the accompanying internet censorship by the government. They don't, however, provide evidence of large-scale use of Tor in Egypt at the time.

14. Cattle, "Digital Tahrir Square."

15. Youmans and York, "Social media and the activist toolkit"; Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017).

16. Haythem Guesmi, "The social media myth about the Arab Spring," *Al Jazeera*, January 27, 2021.

17. Tarik Ahmed Elseewi, "The Arab Spring | A Revolution of the Imagination," *International Journal of Communication* 5 (2011): 1197–1206.

18. In particular, a frequently shared video of Appelbaum (featured in Laura Poitras' documentary *Risk*) casts a negative light on the Tor trainings, depicting him explaining encryption and online anonymity to a room of Tunisian women through crude sexual metaphors.

19. As documented in *Risk* and in reporting on Assange by Andrew O'Hagan in the London Review of Books.

20. Laura Poitras, *Risk* (New York: First Look Media, 2016).

21. As evinced by media appearances, including their regular *State of the Onion* speeches at conferences like the Chaos Communications Congress and Hackers on Planet Earth.

22. Edward Snowden, *Permanent Record* (New York: Metropolitan, 2019).

23. Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Vintage: New York, 2014).

24. Harding, *The Snowden Files.*

25. "'Tor Stinks' presentation—read the full document," *The Guardian*, October 4, 2013.

26. It's worth noting that this is only a single slide deck, produced by one team within a vast organization. Given the segmentation of knowledge and capacities within intelligence services, it may well be that the author was simply unaware of the wider capacities of teams within the Five Eyes to break Tor in different ways.

27. Sarah Myers West, "Survival of the cryptic: Tracing technological imaginaries across ideologies, infrastructures, and community practices," *New Media & Society* 24, no. 8 (August 2022): 1892.

28. With important work being done by Maria Xynou and several other OONI members, as detailed here. "About," Open Observatory of Network Interference, https://ooni.org/about/.

29. Tom Fox-Brewster, "Facebook opens up to anonymous Tor users with .onion address," *The Guardian*, October 31, 2014.

30. "Alec Muffet," Github, https://github.com/alecmuffett/eotk.

31. Roger Dingledine, "Announcing Shari Steele as our new Executive Director," *Tor Project*, December 11, 2015.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

32. Nathalie Marechal, "Use Signal, Use Tor: The Political Economy of Digital Rights Technology" (PhD diss., University of Southern California, 2018).
33. Jason Murdock, "Tor developer Isis Agora Lovecruft publicly accuses the FBI of harassment," *International Business Times*, May 6, 2016.
34. Steven J. Murdoch, "Comparison of Tor datagram designs" The Tor Project, November 7, 2011.
35. Though to be clear, much of the criticism was manifestly disingenuous.

CHAPTER 9

1. Coralie Zaza, "No More Rock Stars: The Challenges of Gendered Hacktivism," April 30, 2017; Mandy Merck, "Masked men: Hacktivism, celebrity and anonymity," *Celebrity Studies* 6, no. 3 (July 2015): 272–287.
2. Appelbaum denies these accounts.
3. Violet Blue, "But He Does Good Work," *Medium*, June 15, 2016.
4. Anna Catherin Loll, "Power, secrecy and cypherpunks: how Jacob Appelbaum ripped Tor apart," *The Guardian*, October 11, 2016.
5. Andrea Peterson, "Jacob Appelbaum was an online privacy hero. Then a sex misconduct scandal exploded," *Washington Post*, June 27, 2016.
6. Blue, "But He Does Good Work."
7. Shari Steele, "Statement," *Tor Project*, June 4, 2016.
8. Danny Yadron, "Digital privacy activist Jacob Appelbaum denies colleagues' assault allegations," *The Guardian*, June 6, 2016.
9. Nick Davies, "10 days in Sweden: the full allegations against Julian Assange," *The Guardian*, December 17, 2010.
10. As documented in depth in Nathalie Marechal's PhD thesis.
11. An undrinkable energy drink favored by the hacker underground.
12. See Christina Dunbar-Hester, *Hacking Diversity: The Politics of Inclusion in Open Technology Communities* (Princeton: Princeton University Press, 2019) for a rich discussion of the wider movements around inclusion in open source over this period.
13. Cory Doctorow, "What happened when we got subpoenaed over our Tor exit node," *Boing-Boing*, August 4, 2015.
14. One of these technologies, entering its fifth year and increasingly mature at the time of writing, is *Cwtch*, an anonymous messenger with Tor built into its heart, developed by Sarah Jamie Lewis' Open Privacy Research Society.

CHAPTER 10

1. Isabela Fernandes, "COVID-19's impact on Tor," *Tor Project*, April 17, 2020.
2. Especially the Eternity Service, in its guise as Wikileaks, Bitcoin, and Tor itself.

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

3. Ben Collier, Gemma Flynn, James Stewart, Daniel Thomas, "Influence government: Exploring practices, ethics, and power in the use of targeted advertising by the UK state," *Big Data & Society*, February 24, 2022.
4. Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (Public Affairs, 2018).

AFTERWORD

1. Nathalie Marechal, PhD thesis (forthcoming).
2. Daniele Pizio, "Forced to live side by side. Power, privacy and conflict in the Tor network," PhD diss. (University of Leicester, 2021).

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Index

Abuse, in system administration, 3, 6, 8, 18, 83–88, 95, 113, 124, 125
Al Jazeera, 155
Anarchism, 73, 81, 89, 90, 127, 161, 162, 167, 170, 174, 206
Anderson, Ross, 52–55, 107, 208. *See also* Eternity Service
Anonymity
  models, 48, 103, 114
  projects, 30, 32, 53–56, 60, 79, 96, 204
  technical concept, 16, 40, 42–49, 59, 63–75, 85, 88, 99, 117, 118, 127, 128–130, 159, 165, 199
  value, 15, 18, 48, 133, 161, 166
  sets, 64–66
Appelbaum, Jacob
  allegations and expulsion, 173–177
  conflicts with law enforcement, 169
  digital trainings, 151–152
  engagement with press, 154–157, 170
Arab Spring
  events of the, 149, 153–156
  Tor's involvement in the, 5, 154, 158, 160, 201, 204
ARPANET, 26, 32. *See also* Eras of the internet, internet origins (1950s–1960s)
Artificial intelligence, 28, 198
Assange, Julian, 107, 108, 114, 129, 156, 157, 176, 188
Attack brainstorming, 67–69, 186–187
Autonomous System, 12, 67, 69

Backdoor (software exploit), 36, 47, 108, 112
Barlow, John Perry, 98
Bike shed problem, 114–115
Blankenship, Loyd, 98
Blue, Violet, 175
Bogatov, Dmitri, 141
BoingBoing, 184
Border Gateway Protocol, 12. *See also* Autonomous System
Botnets, 5, 88, 136, 203. *See also* Cybercrime
Bouazizi, Mohamed, 153. *See also* Arab Spring
Brass Horn (internet service provider), 89
Brave Browser, 194
Broadcasting Board of Governors, 103
Bugfixing (engineering practice), 22, 74, 96, 109, 118, 133, 187
Bulletin boards, 32, 33, 97, 98
Bulletproof hosting, 136

Calyx Institute, 88
Cambridge Analytica scandal, 14
Cambridge Computer Lab, 57, 58, 103, 117, 118
Capitalism, 34, 112, 150. *See also* Globalization; Neoliberalism

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Censorship
circumvention of, 1, 2, 7, 15, 16, 55, 57, 79, 85, 93, 94, 103, 104, 118, 124, 127, 128, 130, 139, 144, 150, 152, 154, 161, 162, 163, 165, 170, 171, 189, 190, 195, 196, 199, 204
of Tor, 3, 11, 55, 86, 135, 139, 152, 163, 170, 196
Central Intelligence Agency (CIA), 27, 39, 42, 55, 102, 103, 108, 204
Chaos Communications Congress, 80, 96, 106, 107, 138, 145, 162, 165, 166, 171, 175, 177
Chaum, David, 29, 30, 40, 128
China, 17, 35, 60, 103, 150, 165, 170, 171, 196, 205
Clark, Erinn, 120, 161, 162
Clinton Administration, 35, 103
Clipper chip, 36. *See also* Crypto Wars
Cold War, 7, 25, 26, 27, 34, 102, 126, 127, 170, 185, 201
Coleman, Gabriella, 29
Cryptocurrency
Bitcoin, 128–130
communities around, 133, 136, 198, 200, 202
conceptual roots of, 128, 130
Ethereum, 200
Zcash, 161, 199
Cryptography
academic research concerning, 29, 96, 101, 102, 105, 115, 160, 161, 162, 177,
encryption tools using, 30, 32, 35, 36, 40, 81, 114, 127, 130, 188, 199, 206
military applications of, 23, 25, 26, 46, 92, 96, 108, 137
models for assessing, 48, 64–66, 70–75
postquantum, 188
Crypto Wars, 4, 36, 37, 98, 145, 150
Cuba, 162, 163
Cult of the Dead Cow, 152, 175
Cybercrime
as a service, 134–135
communities, 32, 79, 134–136, 138
media representations of, 5, 6
tools for, 203
Cybernetics, 34. *See also* Neoliberalism
Cypherpunks
collaboration between Naval Research Laboratory and, 43–50
community, 29–32
mailing list, 30

Danezis, George, 118
Dark Net. *See* Dark Web
Dark Web
child abuse on the, 139–140
cybercrime groups on the, 134–137
drug markets using the, 3–6, 22, 23, 131–134, 139, 142, 143, 144, 182 (*see also* Silk Road, The [cryptomarket])
in fiction, 3, 6, 139
law enforcement takedowns of, 132, 138
media representations of, 1, 3, 6, 101, 107, 112, 125, 131, 139, 146, 203
Decentralization, 15, 17, 19, 20, 26–28, 31, 34, 35, 38, 48, 49, 52, 53, 56, 59, 72, 89–92, 116, 117, 126–129, 140, 180, 181, 198, 199
Deep web, 124
DEFCON (conference), 80, 182
Democracy, 7, 15, 17, 31, 33, 34, 81, 85, 95, 102, 145, 146, 149–164, 167, 206
Determinism, 19, 34, 150, 155
Diesel, Vin, 84, 85
Digital Defenders Partnership, 178
Digital Millennium Copyright Act (DMCA), 84, 85, 87
Dingledine, Roger, 53–59, 74, 75, 79, 86, 96, 97, 99–104, 108, 120, 126, 152, 157, 182
Doctorow, Cory, 184, 185
Do-ocracy, 116, 175

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Dot-com boom, 23, 51, 134, 198
Dulles, Allen, 102

Electromagnetic Field (conference), 80
Electronic Frontier Foundation (EFF), 97–100, 103–104, 143, 150, 151
Entrepreneurial culture, 34, 98, 101, 105, 131, 133–135
Eras of the Internet
  COVID-19 pandemic (2020–2022), 193–208
  early internet cultures (1970s–1980s), 28–33
  early 2000s (2000–2005), 51–96, 100–101
  internet origins (1950s–1960s), 26–28
  late 2000s (2006–2009), 100–122
  Polycrisis (2021–present), 194–208
  post-Snowden period (2013–2019), 157–191
  social media boom (2009–2012), 123–157
  Web commercialization (1990s), 33–50, 97–99
Espionage, 1, 2, 13, 21, 26, 39, 60, 62, 63, 65, 66, 81, 91, 102, 108, 110, 113, 135, 137, 151, 158, 159, 160, 184, 195, 204
Eternity Service, 52–55, 107, 208

Far right movements, 90, 125, 166, 170, 182
Federal Bureau of Investigation (FBI), 81, 98, 126, 132, 147, 169, 184
Feminism, 90, 162, 166, 167, 170, 174, 177
Fernandes, Isabela, 168, 189, 190, 191
Filasto, Arturo, 162–163
Filesharing
  BitTorrent, 52–54, 59, 84, 85
  LimeWire, 52, 59
  Napster, 52–54, 59
  technologies, 32, 52–56, 59, 75, 83–86
Fingerprinting, 13, 14
Firefox, 2, 119, 147, 168, 187, 194
Five Eyes (intelligence-sharing partnership), 56, 158–160, 204
Five Ians, 56, 204
Free and open source software (FOSS). *See* Open source software
Freedom Network (Zero-Knowledge Systems), 52, 53, 56, 70
Freedom of the Press Foundation, 178
Free Haven, 54–57, 74, 107, 108, 126
FUD (fear, uncertainty, and doubt), 112

Germany, 80, 141, 162, 169
Globalization, 4, 5, 19, 32–35, 51, 52, 73, 86, 150
Goldberg, Ian, 56, 104, 117
Goldschlag, David, 37, 39
Google, 13, 58, 106, 124, 142
Government domestic digital influence, 14, 153
Greenstadt, Rachel, 58, 74
Greenwald, Glen, 158
Gulf War (Operation Desert Storm), 39

Hackers
  conferences, 24, 43, 45, 56, 57, 79–81, 90, 97, 106, 156, 160, 162, 166, 174, 177, 180
  ethic, 28, 94, 135
  in fiction, 6, 29, 32, 139
  misogyny and, 95, 174, 175, 177
  moral genres of, 29–33
  political activism of, 15, 28, 30, 31, 33, 36, 135, 151–152, 156, 160–161, 173–174
  political agnosticism of, 31–32, 93–94
  script kiddies, 135
  underground communities, 4, 28, 29, 32, 33, 79, 80, 88, 92, 97–99, 106, 112, 120, 129, 134–138, 144, 152, 153, 156, 160, 173, 174
Hackers on Planet Earth (conference), 80
Harm
  online, 5, 6, 9, 11, 95, 138, 139, 140, 145, 182, 203, 205 (*see also* Cybercrime)
  reduction (drug policy), 134

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Hayden, Michael, 61. *See also* National Security Agency; Metadata; Tor, adversaries of, global passive adversary
Helby, Jennifer, 164
Hierarchy (social structure), 15, 27, 109, 116, 137, 155
Human rights, 3, 38, 53, 81, 91, 95, 99, 100, 102, 105, 146, 164, 168, 172, 181, 182, 184, 200, 201

Identity (online), 37, 38, 40–42, 124, 127, 128, 130, 133, 141
Information Hiding Workshop, 41, 45, 74, 117. *See also* Privacy Enhancing Technologies Symposium
Infrastructure
  control points in, 20, 27, 38, 41, 158, 159, 205, 206
  maintenance of, 21, 24, 77, 89, 95, 96, 109, 140, 188, 195, 197, 204
  and power, 1, 10, 19–24
International Broadcasting Bureau (IBB), 102, 103
International Corporation for Assigned Names and Numbers (ICANN), 35
Internet, infrastructural design of, 10–14, 25–28
Internet freedom activism, 72, 73, 90, 93, 138, 150, 166, 172, 201
Internet Freedom Festival, 165–166
Internet of Things, 194
Internet service providers (ISPs), 11–12, 14, 38, 39, 67, 83–90, 126, 140, 141, 148
Iraq War, 130
Italy, 162
I2P (anonymity network), 124

Johnson, Damian, 120

Komlo, Chelsea, 161, 188

Learmonth, Ian, 106
Lee, Linda, 189
Levien, Raph, 45
Lewis, Sarah Jamie, 133
Lewman, Andrew, 105, 152, 169
LGBTQ rights, 189, 201
Liberty Reserve, 128
Loesing, Karsten, 106
Lovecruft, Isis, 161, 163, 169, 188
Lucky Green (cypherpunk), 58, 70

Mailing lists
  cypherpunks, 30 (*see also* Cypherpunks)
  or-dev, 58, 67–69, 74, 86
  tor-dev, 185
  tor-talk, 84
Manning, Chelsea, 61, 129–130
Massachusetts Institute of Technology (MIT), 53–55, 74
Mathewson, Nick, 53, 54, 55, 74, 75, 99–104, 120, 152
Media Democracy Fund, 178
Metadata, 38–41, 61, 132, 195
Military-academic culture, 23, 25–28, 36, 37–49, 54, 60, 71–75, 115, 170, 206
Mixmaster, 55
Mixminion, 52, 53, 55, 79
Mixnets, 30, 40, 47, 48, 53, 55, 56, 62, 63, 128
Moria Research Labs, 100
Muffett, Alec, 165
Murdoch, Steven, 117–120
Muslim Brotherhood, 155. *See also* Arab Spring

Nakamoto, Satoshi, 128
National Crime Agency (NCA), 138
National Endowment for Democracy, 154
National Science Foundation, 33, 178
Naval Research Laboratory (NRL), 3, 37–50
Neoliberalism, 33–35. *See also* Globalization

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Nerad, Shava, 100–105
Network (structural concept), 1, 7, 12, 13, 17–21, 26–27, 34–35, 41, 48, 71–73, 91, 128, 137, 138, 150, 186
NFT (Nonfungible tokens), 199–202. *See also* Cryptocurrency; Web3

Occupy Wall Street, 155
Omidyar Foundation, 103–104
Onion Routing
  design, 2, 41–43
  NRL roots, 36, 40–50, 204
OnionScan, 133
Online subcultures, 25
OpenNet Initiative, 118
Open Observatory of Network Interference, 162–164
Open source software, 31–32, 109–115

Padding traffic
  initial design in Tor for, 47, 63–71, 196
  netflow, 185–186
Palfrader, Peter, 117
Patriarchy, 17, 18, 139
Perry, Mike, 83
Pfajfar, Matej, 58
Poitras, Laura, 157, 158
Privacy
  in context, 18
  critique of concept of, 9
  cultural specificity of, 15–18
  in digital society, 9–24
  in liberal politics, 7, 15–17, 29, 33–35, 73, 81, 93, 95, 155–157, 161, 162, 168, 171, 176, 198–200, 202, 206
  in liberational politics, 17, 18, 28, 73, 106, 161, 167, 168, 170, 202, 203, 205
  in libertarian politics, 4, 17, 28, 30, 32, 73, 81, 85, 89, 91, 91, 94, 96, 98, 99, 119, 127, 129–133, 157, 160, 161, 170, 171, 173, 177, 181, 183, 198, 199, 206
  relationship with security, 26, 36, 38, 42, 47–49, 61–67, 70–72
  role in civilizing process, 16
  as a service, 77, 92–96, 120–121, 143–144, 170–172, 183–184, 197, 200
  as a structure, 71–75, 109, 121, 144–147, 166, 189, 190, 194–197
  as a struggle, 95, 149, 161, 166–168, 200–206
Privacy Enhancing Technologies Symposium, 56, 74, 96, 105, 117, 165
Privacy worlds concept, 21–23
Privacy worlds, of Tor
  activist, 95, 149, 161, 166–168, 200–206 (*see also* Privacy, as a struggle)
  engineer, 71–75, 109, 121, 144–147, 166, 189, 190, 194–197 (*see also* Privacy, as a structure)
  maintainer, 77, 92–96, 120–121, 143–144, 170–172, 183–184, 197, 200 (*see also* Privacy, as a service)

Radicalization, 137
Radio Free Asia, 103. *See also* Soft power
Radio Free Europe, 7, 102, 103. *See also* Soft power
Ransomware, 136
Reed, Mike, 37, 39
Reilly, Karen, 175
Reputation Technologies, 57
Resilience, 27, 38, 67
Rockstars, in hacker subculture, 154, 173, 177, 180
Russia, 3, 7, 41, 61, 62, 102, 108, 126, 140, 141, 150, 158, 189, 196, 200, 201, 205, 207
Rust (programming language), 199

Sassaman, Len, 118
Schneier, Bruce, 54, 103, 104
Science fiction, 29, 52

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Secrecy, 16, 26, 110
SecureDrop, 164–165
Security
  academic research concerning, 109–114
  defensive, 112
  infosec community, 111–112
  offensive, 111
  OPSEC (operational security), 44, 111
September 11th attacks on the USA, 51, 158. *See also* War on Terror
Shubina, Anna, 84
Side channels
  concept of, 40, 187, 188, 196
  Pentagon Pizza Channel example, 39–40
Silk Road, The (cryptomarket), 131–132
Snowden, Edward, 61, 157–161
Social media platforms, 4, 23, 25, 51, 124, 125, 136, 139, 149, 153, 154, 155, 158, 159, 160, 164, 165, 195, 197, 198, 203
Social Worlds theory, 21–24
Soft power
  cold war, 102–104
  digital democracy, 149–154, 158, 161, 162
  infrastructural (*see* Infrastructure, and power)
  US statecraft, 4, 7, 35, 93, 108, 127, 137, 149, 155–156, 160, 171, 201, 204–206
Standardization, 75, 105, 118, 147, 152, 165, 190, 194, 195
Steele, Shari, 98, 99, 104, 150, 169, 177
Surveillance
  commercial, 1–7, 10–16, 23, 24, 194–195 (*see also* Tracking)
  nation state, 1–7, 9, 13, 16, 30, 31, 35, 39, 46, 53, 61, 90, 92, 94, 98, 128, 132, 137, 147, 152, 158–160, 162–165, 186, 195, 196, 201
Syverson, Paul, 37, 39, 56–58, 66, 67, 75

Targeted advertising, 13–14, 153, 195
Techno-dystopianism, 28, 30, 150, 205
Techno-utopianism, 4, 5, 15, 20, 28–31, 54, 73, 75, 90, 98, 107, 125, 131, 133, 150, 151, 161, 199, 206
Terrorism, 3, 5, 6, 23, 51, 66, 137, 139, 142, 158
Threat modeling, 59–71. *See also* Tor, adversaries of; Tor, technologies of
Tor, adversaries of
  global active adversary, 62, 64
  global passive adversary, 41, 44, 48, 61, 62, 64, 67, 68–71, 159, 184
  roving, 40, 62, 63, 66, 67, 108
  security services, 159, 186, 195, 196
Tor, chronology of
  early design discussions (2001–2003), 51–75 (*see also* Tor, technologies of, design discussions)
  first release (2003), 74–75
  funding and institutions (2006–2010), 97–117
  growth of the relay network (2003–2007), 77–96
  invention of Tor Browser (2008), 118–120
  move into activism (2010–2016), 149–172
  NRL roots (1995–2000), 37–50
  Onion Dinner (1997), 45–46
  professionalization (2015–2020), 167–191
  rise of the Dark Web (2011–2015), 123–148
Tor, political relevance of
  as a neutral tool, 77, 92–96, 120–121, 143–144, 170–172, 183–184, 197, 200 (*see also* Privacy, as a service)
  as a social movement, 95, 149, 161, 166–168, 200–206 (*see also* Privacy, as a struggle)
  as a structural intervention, 71–75, 109, 121, 144–147, 166, 189, 190, 194–197 (*see also* Privacy, as a structure)
Tor, technologies of
  Arti, 199
  design discussions, 58–74, 184–190
  directory authorities, 78

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Hidden Services (*see* Tor, technologies of, Onion Services)
Nyx, 120
Onion addresses, 124, 126, 127
Onion services, 125–128
origins of name, 60
pluggable transports, 170, 190
rendezvous points, 126, 127
reproducible builds, 120
Snowflake, 190, 196, 201
Tor Browser, 1, 2, 14, 21, 78, 117, 117–120, 127, 132–133, 142, 144, 164, 187, 189–191, 194, 199, 208
user design models, 4, 60–61, 67–68, 189
Tor, vulnerabilities of
browser, 22, 74, 96, 109, 118, 133, 187 (*see also* Bugfixing)
hacking core infrastructure, based on, 40, 62, 63, 66, 67, 108 (*see also* Tor, adversaries of, roving)
malicious relays, 78, 115, 183
traffic analysis attacks, 11, 48, 62, 63, 69, 184–186 (*see also* Tor, adversaries of)
Tor relay network
centralization of, 89–91 (*see also* Tor relay network, network diversity)
law enforcement issues, 140–144
network design, 2, 77–96
network diversity, 60, 66, 67, 89–91
operator exit policies, 85–88
operator maintenance practices, 2, 83–88, 120, 143–144
Tor Project
activism by, 149–172 (*see also* Internet freedom activism)
board of directors, 104, 121, 161, 177, 178, 181
funding of, 3, 99–105, 178–180
media strategy of, 101, 102, 105, 121, 146–148, 155–157, 166–169, 181–183
professionalization, 168–170, 177–182
Tor Social Contract, 181, 182
Tor user communities
abuse by cryptomarkets (*see* Cryptomarkets)
abuse by filesharers (*see* Filesharing)
circumventing censorship in authoritarian nations (*see* Censorship, circumvention of; Soft power, digital democracy)
cryptocurrency projects, 133, 136, 198, 200, 202 (*see also* Cryptocurrency, communities around)
hacker communities, 79–82, 90–91, 105–107
human rights activists, 97–99, 104–105
journalists, 158, 163–166, 170, 182
outreach by Tor, 104, 137, 163, 169, 182, 189
privacy enthusiasts, 74, 75
social design of Tor community, 108–117, 187–188
Traceability, 38, 61, 63, 68, 72, 130, 131, 138
Tracking, 2, 13, 14, 66, 69, 83, 128, 130, 147, 161, 164, 187, 194, 195
Transparency, 82, 113–115, 181
Trump, Donald, 164, 180, 183
Trust
in anonymous environments, 57, 138
in Tor by users, 42, 47, 66, 67, 78, 79, 82, 109–113, 188, 189

UK Government Communications Headquarters (GCHQ), 27, 137–138, 159
Ukraine, 200–201
Ulbricht, Ross, 131, 132
Usability
advanced models, 188–188
user interface, 118–121, 190
latency, 47, 71, 88, 104, 119, 123, 137, 152, 159, 179, 196
USENIX conference, 74, 79, 88
US National Security Agency (NSA), 46, 157, 158, 159, 204

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024

Web3, 197–200
Western Union, 128
Wikileaks
  conflicts with government, 156, 164, 181
  links with Tor, 107, 108, 152, 156, 157
  Manning leaks, 129–130 (*see also* Manning, Chelsea)
  US Embassy diplomatic cables leak, 107–108
Wikipedia, 85
Workshop on the Economics of Information Security (WEIS), 74, 103
Wozniak, Steve, 98

Yard, Itzel, 200

Zwiebelfreunde, 88

Downloaded from http://direct.mit.edu/books/book-pdf/2362316/book_9780262378925.pdf by guest on 18 November 2024